1037
Y3.G74/6:P93/2
Pt. 2

PRIVACY

THE COLLECTION, USE, AND COMPUTERIZATION OF PERSONAL DATA

DOCUMENTS
APR 3 1975
APR 3 1975
KANSAS STATE UNIVERSITY
THE LIBRARY
KANSAS STATE UNIVERSITY
KSU LIBRARIES
A11900 929993

JOINT HEARINGS

BEFORE THE

AD HOC SUBCOMMITTEE ON PRIVACY AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON GOVERNMENT OPERATIONS

AND THE

SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

NINETY-THIRD CONGRESS

SECOND SESSION

ON

S. 3418, S. 3633, S. 3116, S. 2810, S. 2542

JUNE 18, 19, AND 20, 1974

PART 2

Printed for the use of the Committee on Government Operations and the Committee on the Judiciary

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PRIVACY

THE COLLECTION, USE, AND COMPUTERIZATION OF PERSONAL DATA

JOINT HEARINGS

BEFORE THE

AD HOC SUBCOMMITTEE ON PRIVACY AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON GOVERNMENT OPERATIONS

AND THE

SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

NINETY-THIRD CONGRESS

SECOND SESSION

ON

S. 3418, S. 3633, S. 3116, S. 2810, S. 2542

JUNE 18, 19, AND 20, 1974

PART 2

Printed for the use of the Committee on Government Operations and the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

37-583 O WASHINGTON : 1974

COMMITTEE ON GOVERNMENT OPERATIONS

SAM J. ERVIN, JR., North Carolina, *Chairman*

JOHN L. McCLELLAN, Arkansas
HENRY M. JACKSON, Washington
EDMUND S. MUSKIE, Maine
ABRAHAM RIBICOFF, Connecticut
LEE METCALF, Montana
JAMES B. ALLEN, Alabama
LAWTON CHILES, Florida
SAM NUNN, Georgia
WALTER D. HUDDLESTON, Kentucky

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
EDWARD J. GURNEY, Florida
WILLIAM V. ROTH, JR., Delaware
BILL BROCK, Tennessee

ROBERT BLAND SMITH, JR., *Chief Counsel and Staff Director*
JANET GAY HOLLIDAY, *Chief Clerk*
ELI E. NOBLEMAN, *Counsel*
W. P. GOODWIN, JR., *Counsel*
J. ROBERT VASTINE, JR., *Minority Counsel*
BRIAN CONBOY, *Special Counsel for the Minority*
W. THOMAS FOXWELL, *Staff Editor*
FREDERICK N. MCCLINTOCK, *Editorial Assistant*

AD HOC SUBCOMMITTEE ON PRIVACY AND INFORMATION SYSTEMS

SAM J. ERVIN, JR., North Carolina, *Chairman*

HENRY M. JACKSON, Washington
EDMUND S. MUSKIE, Maine
ABRAHAM RIBICOFF, Connecticut
LAWTON CHILES, Florida
SAN NUNN, Georgia

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
WILLIAM V. ROTH, JR., Delaware
BILL BROCK, Tennessee

MARCIA J. MACNAUGHTON, *Staff Director*
JAMES DAVIDSON, *Special Counsel*
Dr. ALAN F. WESTIN, *Special Consultant*
Dr. CHRISTOPHER H. PYLE, *Consultant*
MARK BRAVIN, *Consultant to the Minority*

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

JOHN L. McCLELLAN, Arkansas
SAM J. ERVIN, JR., North Carolina
PHILIP A. HART, Michigan
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
QUENTIN N. BURDICK, North Dakota
ROBERT C. BYRD, West Virginia
JOHN V. TUNNEY, California

ROMAN L. HRUSKA, Nebraska
HIRAM L. FONG, Hawaii
HUGH SCOTT, Pennsylvania
STROM THURMOND, South Carolina
MARLOW W. COOK, Kentucky
CHARLES MCC. MATHIAS, JR., Maryland
EDWARD J. GURNEY, Florida

JOHN H. HOLLOMAN III, *Chief Counsel and Staff Director*

SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

SAM J. ERVIN, JR., North Carolina, *Chairman*

JOHN L. McCLELLAN, Arkansas
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
ROBERT C. BYRD, West Virginia
JOHN V. TUNNEY, California

EDWARD J. GURNEY, Florida
ROMAN L. HRUSKA, Nebraska
HIRAM L. FONG, Hawaii
STROM THURMOND, South Carolina

LAWRENCE M. BASKIR, *Chief Counsel and Staff Director*
DOROTHY GLANCY, *Counsel*
IRENE R. MARGOLIS, *Professional Staff Member*

CONTENTS

REMARKS BY COMMITTEE MEMBERS

	Page
Senator Ervin	1
Senator Percy	8
Senator Roth	10
Senator Ribicoff	7
Senator Mathias	11
Senator Jackson	14
Senator Javits	52
Senator Brock	173
Senator Bayh	15

WITNESSES

Arnoff, Hon. Stanley, State Senator from Ohio, on behalf of the National Legislative Conference	212
Prepared statement (with attachments)	217
Atkinson, Andrew, Chairman, Projects '74; Committee Superintendent, Regional Computer Center, Ohio, Executive Director, Government Management Information Services	256
Prepared statement	259
Barabba, Vincent A., Director, Bureau of the Census, Department of Commerce	148
Prepared statement	149
Buchen, Philip W., executive director, Domestic Council Committee on the Right of Privacy, accompanied by Douglas W. Metz, deputy executive director	120
Davis, Ruth M., Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Department of Commerce	134
Prepared statement	138
Eastman, Hope, associate director, Washington Office, American Civil Liberties Union	153
Prepared statement	156
Supplemental statement	165
Gabrieli, Dr. Elmer, chairman, Joint Task Group on Ethical Data Centers	345
Goldwater, Hon. Barry M., a U.S. Senator from the State of Arizona	113
Prepared statement	114
Goldwater, Hon. Barry M., Jr., a Representative in Congress from the State of California	23
Hammett, Jerry, deputy director, Department of Administrative Services of Ohio; chairman, National Association of State Information Systems Committee on Security and Privacy	245
Prepared statement	249

Page

Koch, Hon. Edward, a Representative in Congress from the State of New York ... 19
Larson, Dr. Martin A., tax policy consultant, Liberty Lobby, accompanied by Curtis B. Dall, chairman of the board, Liberty Lobby ... 176
Prepared statement ... 182
Litton, Hon. Jerry, a Representative in Congress from the State of Missouri ... 57
Magraw, Daniel, assistant commissioner of administration from Minnesota; past president of the National Association of State Information Systems ... 239
Prepared statement ... 243
Pyle, Prof. Christopher H., assistant professor, John Jay College of Criminal Justice, City University of New York ... 99
Prepared statement ... 104
Richardson, Hon. Elliot L., former Secretary of the Department of Health, Education, and Welfare ... 36, 53
Salett, Stanley J., senior associate, National Committee for Citizens in Education, accompanied by Stuart A. Sandow, associate ... 187
Prepared statement ... 193
Sampson, Hon. Arthur F., Administrator of the General Services Administration ... 294
Prepared statement ... 323
Schiller, Donna, president, League of Women Voters of Illinois, accompanied by Doris Bernstein, vice president ... 335
Prepared statement ... 337
Schmidt, Richard M., Jr., general counsel, American Society of Newspaper Editors ... 167
Prepared statement ... 171
Trigg, Charles, assistant director, National Association of State Information Systems ... 252
Prepared statement ... 254
Whitehead, Clay, Director, Office of Telecommunications Policy, Executive Office of the President ... 332
Westin, Dr. Alan, professor of public law and government, Columbia University ... 65
Prepared statement ... 82

LEGISLATION

Remarks of Senator Ervin on introducing S. 3418, a bill to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State, and local governments, and other organizations regarding such information, and for other purposes ... 351
Remarks of Senator Percy at time of introduction of S. 3418 ... 355
Text of S. 3418 ... 357
Remarks of Senator Ervin on introducing S. 3633, a bill to protect the constitutional right of privacy of individuals concerning whom identifiable information is recorded by enacting principles of information in furtherance of articles I, III, IV, V, IX, X, and XIV of amendment to the U.S. Constitution ... 377
Remarks of Senator Kennedy at time of introduction of S. 3633 ... 378

Page

Text of S. 3633 380
Remarks of Senator Hatfield on introducing S. 3116, a bill to protect the individual's right to privacy by prohibiting the sale or distribution of certain information 402
Text of S. 3116 404
Remarks of Senator Bayh on introducing S. 2542, a bill to protect the constitutional right of privacy of those individuals concerning whom certain records are maintained, and for other purposes 407
Text of S. 2542 409
Text of S. 2810, a bill to protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, V, IX, X, and XIV of the U.S. Constitution, introduced by Senator Goldwater 416
Announcement of Joint Legislative Hearings, by Senator Ervin, June 11, 1974 1603
Proposed Administration bill (OMB draft) 441

AGENCY COMMENTS

Central Intelligence Agency 486
Civil Service Commission 447
Commerce, Department of 450
Comptroller General 454
Defense, Department of 456
Federal Trade Commission 460
Health, Education, and Welfare, Department of 472
Justice, Department of 474
Office of Management and Budget 440
Postal Service 484
Securities and Exchange Commission 478
Treasury, Department of 480

STATEMENTS

Congressional Members

Biden, Hon. Joseph R., Jr., a U.S. Senator from the State of Delaware 487
Buckley, Hon. James L., a U.S. Senator from the State of New York 487
Hatfield, Hon. Mark O., a U.S. Senator from the State of Oregon 209
Horton, Hon. Frank, a U.S. Representative from the 34th Congressional District of New York (with enclosures) 489

General

American Life Insurance Association 515
American Mutual Insurance Alliance 519
American Petroleum Credit Association 519
Associated Credit Bureaus, Inc 520
Association of American Publishers, Inc 524
American Bankers Association 525
Branscomb, Lewis M., IBM vice president and chief scientist 673
Byrley, Charles A., representing the National Governors' Conference 271
California Bankers Association 526

Page

Chase Manhattan Bank 528
Countryman, Vern, professor of law, Harvard Law School 1392
Direct Mail/Marketing Association, Inc., John Jay, Daly, senior vice president 529
Dumont, Matthew P., M.D., Assistant Commissioner for Drug Rehabilitation, Department of Mental Health, Commonwealth of Massachusetts 557
Federal Government Accountants Association 581
Holloway, Guy L., president, Commercial Services, Inc., Madison Heights, Mich. (on behalf of said company), and the Associated Reporting Companies (a national association) 583
International Business Machines Corporation 667
Jarocki, Stanley Robert, Sterling, Va 583
Johnstone, Dr. John, Jr., chairman, Patient Care Appraisal Committee, St. Joseph Hospital, Kirkwood, Mo 587
Joint Task Group on Essential Health Data Systems 346
Magazine Publishers Association, Inc 590
Makley, Janet, Dayton, Ohio 591
Malany, LeGrand L., Springfield, Ill 592
Miller, Arthur R., professor of law, Harvard University 593
National Bank Americard 605
National Federation of Federal Employees 622
National Grange 350
National Newspaper Association 625
National Retail Merchants Association 628
O'Brien, Fred Burns, J.D., Washington, D.C 636
Parker, Donn B., senior information processing analyst, Information Science Laboratory 643
Patrick, Robert L., computer specialist 644
Pipe, G. Russell, Amsterdam, Holland 679
Retail Credit Company of Atlanta, Ga 647
Ryan, Bernard, Washington State Senate Judiciary Committee, research analyst 655
Sears, Roebuck and Co 656
Shattuck, John F., staff council, American Civil Liberties Union Foundation 717
Shoup, Guy W., Wyatt, Gerber & Shoup, attorneys at law, New York City 658
Skolfield, Thomas J., director of information and evaluation, city of Portland, Maine 647
Sun Oil Co 663
TRW Credit Data 664
Walker, Hon. Dan, Governor of State of Illinois 343
Wheeler, Hon. Charles B., Jr., mayor, Kansas City, Mo 612

REPORTS AND STUDIES

"Federal Data Banks and Constitutional Rights," summary and conclusions of a study of data systems on individuals maintained by agencies of the U.S. Government, prepared by the staff of the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 1974 723
"Records, Computers, and the Rights of Citizens," excerpt from Report of the Secretary's Advisory Committee on Automated Personal Data Systems (DHEW publication No. (os)83-97), U.S. Department of Health, Education, and Welfare, July 1973 781

"Databanks in a Free Society—Computers, Record-Keeping and Privacy," excerpt from Report of the Project on Computer Databanks of the Computer Science and Engineering Board, National Academy of Sciences, by Alan F. Westin, Project Director and Michael A. Baker, Assistant Project Director ..... Page 1057
"Legal Aspects of Information Systems," excerpt from report by Federal Council of Science and Technology, Committee on Scientific and Technical Information 1125
"Social Security Number Task Force," report to the Commissioner, Social Security Administration, Department of Health, Education, and Welfare, May 1971 1156
"The Preservation of Privacy," excerpt from report by the United Presbyterian Church of the United States 1283
National Conference of Catholic Bishops 607
Freedom of Information Center Report No. 291: "Access to Personal Data Files," from the School of Journalism, University of Missouri at Columbia, October 1972 1314
National Governors Conference Report on Individual Privacy 273
Council of Europe, Committee of Ministers, Privacy resolution 1729
Administrative Conference of the United States; "Interagency Transfer of Information in Individually Identifiable Form," by Prof. Alex Bell, September 1973 2301
Recommendations, 1974 2295

LAW REVIEW ARTICLES

American University Law Review, "Privacy: Establishing Restrictions on Government Inquiry," by G. Russell Pipe 680
Duke Law Journal, "Computers and Privacy: a Proposal for Self-Regulation," by Edward J. Grenier, Jr 1623
Columbia Human Rights Review, "The First Amendment: A Living Thought in the Computer Age," by Senator Sam J. Ervin 1339
Yale Law Journal, "Privacy in the First Amendment" 1374
Texas Law Review:
"The Diminishing Right of Privacy: Personal Dossier and the Computer," by Vern Countryman 1392
"A Different View of Privacy," by Albert W. Alschuler 1428
"The Diminishing Right of Privacy: A Rejoinder," by Vern Countryman 1437
University of Illinois Law Forum:
"Privacy and Government Investigations," by Senator Sam J. Ervin 1439
"The Dossier Society," by Arthur R. Miller 1456
"Privacy and the Poor," by Michael Harrington 1470
Journal of Public Law, "The Fair Credit Act: A Legislative Overview," by Robert M. McNamara 1481

STATUTES AND DECISIONS

Administrative Procedure Act (5 U.S.C. 500–559) 1516
Freedom of Information Act (5 U.S.C. 552) 1518

Computer Laws: Page
Authorizing a Federal Telecommunications Fund (40 U.S C. 757) 1525
"The Brooks Act" (40 U.S.C. 759) providing for procurement, maintenance, operation, and utilization of ADP equipment 1526
Public Law 91-508:
Requiring banks to maintain certain records and report certain transactions 1529
The Fair Credit Reporting Act 1541
Federal Reports Act 1555
Law relating to Federal records management (44 U.S.C. chs. 29, 31, 33, and 35) 1551
U.S. v. *Rumley* (345 U.S. 41 (1953)) 1567
Wisconsin v. *Constantineau* (400 U.S. 433 (1971)) 1584
Lamont v. *Commissioner of Motor Vehicles* (269 Fed. Supp. 880) 2247
Tarver v. *Smith* (402 U.S. 1000) 1597

CONGRESSIONAL RECORD EXCERPTS CONTAINING REMARKS ON PRIVACY BY MEMBERS OF CONGRESS

SENATE REMARKS:
Ervin, Hon. Sam J., Jr.:
"Privacy and Government Information Systems," June 11, 1974, announcement of hearings 1603
"Computers, Data Banks, and the Bill of Rights," February 8, 1971 1606
"Federal Data Banks and the Bill of Rights," September 8, 1970 1609
"Computers and Individual Privacy," November 10, 1969 1614
"International Declaration of Principle on Computers and Privacy," October 10, 1972 1633
Percy, Hon. Charles H.: "Threat to Privacy," June 17, 1974 1635
HOUSE OF REPRESENTATIVES:
Remarks by Members during Special Order on Privacy, April 2, 1974, including excerpts from remarks by 200 members and research information and other data on privacy issues (submitted by Congressman Koch as exhibit) 1642

SURVEY OF GOVERNORS AND STATE ATTORNEYS GENERAL ON S. 3418, PRIVACY, AND STATE LAWS AND PROGRAMS

State of:
Alabama 1820
Arkansas 1821
California 1822
Connecticut 1889
Florida 288, 1890
Georgia 1891
Illinois 289, 343, 1892
Iowa 288
Kansas 1892
Kentucky 1893
Louisiana 1895
Maine 1912
Massachusetts 281
Montana 289

State of—Continued Page
Minnesota 290
Nebraska 1912
Nevada 1912
New Mexico 1913
New York 1923
North Dakota 1928
Ohio 1928
Pennsylvania 1931
South Dakota 1933
Utah 1933
Vermont 1934
Virginia 1936
Washington 1943
Wyoming 1991

MODEL LEGISLATIVE PROPOSAL

National Association for State Information Systems, model legislation for a fair information practices act 263

LETTERS AND COMMUNICATIONS

Ervin, Hon. Sam, Jr., to Hon. Arthur Sampson, Administrator of General Services, June 17, 1974, confirming his appearance as witness and suggesting lines of testimony the committee will consider 293
Buchen, Philip W., executive director, Domestic Council Committee on the Right of Privacy to Senator Ribicoff, June 27, 1974, concerning examples of information the Government considers necessary for public protection 129
Percy, Hon. Charles H., a U.S. Senator from the State of Illinois, to Philip W. Buchen, June 26, 1974, requesting answers to questions concerning privacy, with response 130, 131
Eastman, Hope, associate director, ACLU, to Senator Ervin, June 27, 1974 165
Ervin, Hon. Sam, Jr., to Hon. Arthur Sampson, Administrator of General Services, July 8, 1974, with response to questionnaire regarding new equipment project 308
Ayres, L. S. & Co., to Hon. Birch E. Bayh, Jr., U.S. Senator, July 17, 1974, regarding elimination of social security numbers from credit applications 1994
Letters to Senator Percy from citizens 1995

ARTICLES AND PUBLICATIONS

"A Fight Over Data Banks," editorial from the Washingotn Post, June 18, 1974 30
"Databanks in a Free Society: A summary of the Project on Computer Databanks," by Prof. Alan F. Westin, from Computers and Automation, January 1973 92
"Curb the Computers—Datamania and Privacy," from the (Philadelphia) Evening Bulletin, June 26, 1974 2002
"Controlling the Data Banks," editorial from the Washington Post, July 19, 1974 2002

Page

"New Discrepancies Found in Controller's Accounts," from the New York Times, July 17, 1974 ... 2003
"Police Computer Information Use Increases," from the Washington Post, July 6, 1974 ... 2005
"Latest Police Item: Portable Computer Terminal," by Paul Hodge and Alfred E. Lewis, Washington Post staff writers ... 2007
"Your Life: How Private?" by David Kuhn, reprinted from the Minneapolis Tribune, October 7–12, 1973 (a series) ... 2008, 2019
From the New York Daily News, by Michael Pousner, a series:
"The Rape of Privacy" ... 2019
"How Brian McGraw Was Left for Dead" ... 2021
"Slamming the Door on Snoops: Step 1" ... 2023
"The Information Seekers: Your Privacy Is Their Concern," by John Fialka, from the Washington Star-News, May 25, 1974 ... 2025
"Next: The Cashless Society (But Will You Like It?)", by John Holusha, from the Washington Star-News, June 15, 1974 ... 2029
"Use of Personal-Characterization Coding on Military Discharges Is Assailed," by Peter Kihss, from the New York Times, September 30, 1973 ... 2033
"Living by the Numbers," editorial from the Washington Post, September 12, 1973 ... 2035
"Federal Computers Amass Files on Suspect Citizens—Many Among Hundreds of Thousands Listed Have No Criminal Records—Critics See Invasion of Privacy," by Ben A. Franklin, from the New York Times, June 28, 1970 ... 2036
"Data Banks, Privacy and Society," Ware, Willis H ... 1766
"Multinational Data Banks," Lundale, E. Drake, Computerworld, Jan. 16, 1974 ... 1803
"A Nation of Datamaniacs," Miller, Arthur, Prism, June 1974 ... 1804

PUBLICATIONS OF THE NATIONAL BUREAU OF STANDARDS RELATING TO COMPUTER TECHNOLOGY

"Executive Guide to Computer Security" ... 2041
"Government Looks at Privacy and Security in Computer Systems" ... 2084
"Government Looks at Privacy and Security in Computer Systems," (series 2) by Dr. Ruth M. Davis ... 2137
"The Versatile Computer: It Must Be Controlled (1973)" ... 2132
"Controlling Access to Your Computer May Be Best Selling Point," by Dr. Ruth M. Davis ... 2060
"Guidelines for ADP Physical Security and Risk Management" ... 2081
SOCIAL SECURITY NUMBERS ... 587, 2234
MILITARY RECORDS ... 1647
FARMERS RECORDS ... 1665, 1667
SENSITIVITY TRAINING ... 1787
CENSUS AND STATISTICAL DATA ... 1670
BANK SECRECY ... 1671, 1681

STUDENT RECORDS

Senate remarks by Senator Buckley and others on protection of the rights and privacy of parents and students, questionnaires, and other research material ..... Page 2153
Carey, Sarah, "Students, Parents and the School Record Prison: A Legal Strategy for Preventing Abuses" 1779
Cashman, Charles E., "Confidentiality of Juvenile Court Proceedings" 1748
Divoky, Diane, "Cumulative Records: Assault on Privacy" 1773

MEDICAL RECORDS

Dumont, Dr. Matthew P.:
"CODAP: The Monster Masqurading as a Windmill" 561
"The Computer Sees the Truth But Waits" 563
Other articles concerning medical programs 570, 575, 580
"Ethical Aspects of Medical Confidentially," by LeRoy Walters, Ph. D., director, Center for Bioethics, Kennedy Institute, Georgetown University, Washington, D.C., presented at the Sixth Buffalo Conference on Computers in Clinical Medicine, Niagara Falls, N.Y., June 19, 1974 2226
Resolution from the State of New York, Legislature of Erie County, Jnly 3, 1974 2232
Resolution on "Confidentially: A Release of Privileged Medical Information to Credit Reporting Agency," introduced by the District of Columbia Society on Internal Medicine 2233
Johnson, Hugh B., M.D., letter to Senator Mark Hatfield, September 6, 1974, regarding privacy legislation 2233
Sargent, Francis W., Governor of Massachusetts, letter to Hon. Casper W. Weinberger, Secretary, HEW, July 15, 1974, with attachments 2234
Gabrieli, E. R., M.D., chairman, Joint Task Group on Confidentially of Computerized Medical Records, to Mark Bravin, Government Operations Committee, July 1, 1974, regarding questions submitted 2239
"Privacy and Medical Recordkeeping," by Barbara L. Kaiser 2240
MAILING LISTS 209, 402, 490, 658
Agency Survey 490

FACT SHEETS

Constitutional Rights Subcommittee:
Federal data banks 2252
FEDNET 2253
White House fact sheet on President's address of February 23, 1974, on right of privacy 1813

INDIVIDUAL CASES ILLUSTRATING NEED FOR NEW LAW

Privacy: The right to see one's own file, staff report of Subcommittee on Constitutional Rights 2256
Census questionnaire, a letter to Senator Ervin, with supporting material 2257
Other Individual Cases 1314, 1684, 1686

MISCELLANEOUS

Page

Business Equipment Manufacturers Association (BEMA) response to FCC docket No. 16979, in the matter of Regulatory and Policy Problems Presented by the Interdependence of Computer and Communications Services and Facilities 2288

Remarks by Vice-President Ford, National Computer Conference, May 9, 1974 278

Address by President Nixon, Feb. 23, 1974, on Right of Privacy and Fact Sheet on Privacy 1810, 1813

Secret Service Data Collection (related correspondence) 1619

Health, Education, and Welfare Department Regulations, May 30, 1974, "Protection of Human Subjects" 2209

APPENDIX

LAW REVIEW ARTICLES

4 COLUMBIA HUMAN RIGHTS REVIEW (No. 1) (1972)

The First Amendment: A Living Thought in the Computer Age[1]

By
Sam J. Ervin, Jr.*

Sherwood Anderson wrote words about America as true today as they were in the third decade of this century:

> America ain't cemented and plastered yet. They're still building it. . . . All America asks is to look at it and listen to it and understand it if you can. Only the understanding ain't important either; the important thing is to believe in it even if you don't understand it, and then try to tell it, put it down. Because tomorrow America is going to be something different, something more and new to watch and listen to and try to understand; and, even if you can't understand, believe.

Anyone seeking to understand contemporary America must deal with our national experience with computer technology. They must understand that it has become an essential tool in the "cementing and plastering" of our nation. They must understand that it has at once presented our country its greatest hope and its greatest challenge; keeping faith with our historical heritage and commitment to freedom, while enjoying the fruits of a rich industrialized society under a democratic constitution.

Throughout our nation the people involved with computer technology have charge of a great national resource which will affect the course of our economic and social progress. More important, insofar as it affects the exercise of governmental power and the power of large special interest groups, the new technology may help determine the course of freedom and human rights in our land.

---

* U.S. Senator, North Carolina.

1. Based on an address before the Spring Joint Computer Conference of the Federation of Information Processing Societies, Atlantic City, N.J., May 20, 1971.

In the process, I believe Americans could find wisdom in Sherwood Anderson's advice "to believe" in America. I say this because, as we grasp for the new computer technology and seek theories of systems analysis for our social problems, Americans may tend to forget to look to their own history. Some, in their haste to solve today's problems, may fear to translate America's promise of freedom into the program language of the computer age.

Those who are initiated into the technological mysteries of computer hardware and software may take great pride. Through their deeds and genius they have helped people go to the moon, produce music, create art, conduct off-track betting, run railroads and administer welfare systems. They help maintain our national defense and they keep our economy running. They aid in catching criminals and they establish instant credit. They locate marriage-mates for people and they prejudge elections almost before the votes are cast.

A tape storage system has been described which will make it possible to store a dossier on every living person in the United States and to retrieve any one of them in a maximum of 28 seconds. With such feats to their credit, these people know better than anybody that in the application of their knowledge, they play a major role in the economic and social well-being of our society. They are responsible for bringing to our nation all the wondrous blessing of computer technology, especially scientific methods of processing information.

They can bend these machines to their will and make them perform feats undreamed of ten or even five years ago.

They have a special understanding of the new information flow charts for the vast data systems in our government.

They hold the access code to control over the technology as it affects the individual in our society.

They may hold the key to the final achievement of the rule of law which is the promise of our constitution.

With this body of knowledge, therefore, they bear special responsibility for the preservation of liberty in our country. That they have accepted this responsibility is clear from the *Privacy* themes of many recent conferences of computer professionals, equipment manufacturers, and computer users in the governmental and private sectors.

Their power is not limited to their technical expertise, but is augmented by the sheer numbers in the computer-related professions.

Advertisements on TV, radio, in newspapers, and even on buses daily remind the public of the inducements and rewards of a career in computer and data processing fields.

In the Federal Government, their numbers are growing. An inventory of automatic data processing equipment shows that in 1952

there were probably two computers in government. In 1971, there were 5,961.[2]

In 1960, there were 48,700 man-years used in federal automated data processing functions. This includes systems analysis and design, programming, equipment selection and operation, key punching, equipment maintenance and administrative support. In 1970, there were about 136,504 man-years used in direct ADP work.

A recent illuminating report by the National Association for State Information Systems shows that in 35 states in 1971, over twenty-four and a half thousand people were engaged in ADP. Twenty-eight states together spent 181 million dollars of their budgets on such personnel.[3]

To glance through their professional journals, newspapers and bulletins each month is to be constantly amazed at the breadth and reach of the theories and accomplishments.[4] It also deepens a layman's wonder at the complex language which sometimes defies translation into ordinary English.

For all of these reasons, the general public stands in superstitious awe of the skills and knowledge, the machines and instruments, and the products derived and transmitted by them. For the uninitiated, the computer print-out bears a mystique and an aura of scientific rationality which makes it appear infallible. This is true for most lawyers and probably for most people in political life.

There is a theory abroad today in academic circles that America is divided into two worlds. One of them is the world of science and technology,[5] inhabited by people who are part of a technological and electronic revolution. In the other world are said to live all the rest of the people whose ideas and values are based on an earlier age.

In accordance with their theory, some have tried to stamp the scientist with motives and values different from those of other Ameri-

2. INVENTORY OF AUTOMATIC DATA PROCESSING EQUIPMENT IN THE UNITED STATES FISCAL YEAR 1971, GENERAL SERVICES ADMINISTRATION, at 15. A report providing information on the digital electronic computers installed throughout the U.S. Government, which defines "computer" as a configuration of EDPE components which includes one central processing system concept which recognizes the growing importance of configurations with more than one central processing unit. This report responds to requirements of P.L. No. 89-306, Stat. (Oct. 30, 1965) and S. Doc. No. 15 (1965), REPORT TO THE PRESIDENT ON THE MANAGEMENT OF AUTOMATIC DATA PROCESSING IN THE FEDERAL GOVERNMENT.

3. 1970 NASIS REPORT, INFORMATION SYSTEMS TECHONOLOGY IN STATE GOVERNMENT at 18, developed by the State of Illinois and the National Association for State Information Systems, Council of State Governments.

4. *See generally* COMPUTERWORLD (a weekly periodical servicing the computer community): DATAMATION: DATA MANAGEMENT; and BUSINESS AUTOMATION.

5. *See, e.g.*, Brzezinksi, Between Two Ages, America's Role In The Technotronic Era, although all authors do not engage in such distinctions with the same judgments or purposes.

cans; with goals oriented only toward efficiency or shorn of compassion, or, alternatively, with exclusive ability to determine social priorities. I cannot agree with this analysis, for I believe there is a yearning in every human heart for liberty, and for the freedom to express oneself according to the dictates of conscience. Despite a man's commitment to a chosen profession, he wants the freedom to fulfill himself as an individual and to use his God-given faculties free from the coercion of government.

So I do not believe Americans dwell in two worlds. Regardless of our origins, I believe we share a common heritage and a common destiny in that we are all engaged in searching for freedom. We share, according to the mandates of the Constitution, a common understanding that the best protection for that freedom rests on the limitations on the power of government and on the division of that power.

I cannot agree with such an analysis for another reason. Since the Senate Constitutional Rights Subcommittee began its study of computers, data banks and the Bill of Rights, I have received many letters from computer specialists, systems designers, engineers, programmers, professors and others in the scientific community which prove that despite, and perhaps because of their professions, they share the same concern about invasion of privacy as all other Americans, the same apprehensions about excesses of governmental surveillance and inquiries. Above all, they realize, perhaps better than others, that while the information technology they deal with can extend the intellect of man for the betterment of society, it also extends the power of government a millionfold.[6]

It makes it possible for government to administer more efficiently and to offer vastly better services to the taxpayers.

At the same time, it extends and unifies official power to make inquiries, conduct investigations, and to take note of the thoughts, habits and behavior of individuals. Of course, government has always had such power, but on a much smaller scale than today. Similarly, men possessing the power of government have always had the capacity for bad motives, simple errors or misguided purpose. There have always been problems with errors in the manual files. Now, computers may broadcast the image of these errors throughout a national information system.

---

6. *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. [Feb. 23-25 and Mar. 2-4, 9-11, 15 and 17 (1971)] [hereinafter cited as *1971 Hearings*]. Testimony of Robert Bigelow, attorney, describing concern of professional computer organizations and press, *id.* at 680; Bibliography, lists of public discussions on privacy and computers in the United States and abroad, *id.* at 692 *et seq.*; Testimony of Professor Caxton Foster, University of Mass., Department of Computer and Information Sciences, *id.* at 707.

What the electronic revolution has done is to magnify any adverse effects flowing from these influences on the life of the individual and on his proper enjoyment of the rights, benefits and privileges due a free man in a free society.

I reject the notion of division of Americans on the basis of scientific and technological values. If I had the unhappy and well-nigh impossible task of distinguishing two types of Americans, I believe I would distinguish between those who understand the proper limits and uses of governmental power and those who do not.

However much we try to rationalize decisions through the use of machines, there is one factor for which the machine can never allow. That is the insatiable curiosity of government to know everything about those it governs. Nor can it predict the ingenuity applied by government officials to find out what they think they must know to achieve their ends.

It is this curiosity, combined with the technological and electronic means of satisfying it, which has recently intensified governmental surveillance and official inquiries that I believe infringe on the constitutional rights of individuals.

Congress received so many complaints about unauthorized government data banks and information programs that the Subcommittee undertook a survey to discover what computerized and mechanized data banks government agencies maintain on people, especially about their personal habits, attitudes, and political behavior. We have also sought to learn what government-wide or nation-wide information systems have been created by integrating or sharing the separate data bases. Through our questionnaire, we have sought to learn what laws and regulations govern the creation, access and use of the major data banks in government.[7]

The replies we are receiving are astounding, not only for the information they are disclosing, but for the attitudes displayed toward the right of Congress and the American people to know what Government is doing.

In some cases, the departments were willing to tell the Subcommittee what they were doing, but classified it so no one else could know.[8] In one case, they were willing to tell all, but classified the legal authority on which they relied for their information power.[9]

7. For a sample of questionnaire sent to all agencies and departments with slight alterations, see Letter to Secretary of Defense Melvin Laird, July 20, 1970, *1971 Hearings* at 1182, and to Attorney General Mitchell, June 9, 1970. *Id.* at 1312.

8. *See, e.g.,* State Department response to questionnaire, concerning its "Lookout File." *See* Letter of Sept. 9, 1970 to Subcommittee Chairman from Assistant Secretary of Defense Robert Moot, and list of classified enclosures. *1971 Hearings* at 1186.

9. Navy Department response, Aug. 13, 1970, citing a Roosevelt Executive memorandum assigning responsibilities for intelligence activities. *Id.* at 1201.

37-583 O - 74 - pt. 2 - 2

Some reports are evasive and misleading. Some agencies take the attitude that the information belongs to them and that the last person who should see it is the individual whom it is about.[10] A few departments and agencies effectively deny the information by not responding until urged to do so.[11]

They reflect the attitude of the Army captain who knew Congress was investigating the Army data banks and issued a directive stating:

> The Army General Counsel has re-emphasized the long-standing policy of the Executive Branch of the Government . . . that all files, records and information in the possession of the Executive Branch is privileged and is not releasable to any part of the Legislative Branch of the Government without specific direction of the President.[12]

So, on the basis of this study, and on the withholdings of information from the American people which the Subcommittee has experienced,[13] I have concluded that the claim of the Government departments to their own privacy is greatly overstated. The truth is that they have too much privacy in some of their information activities. They may cite the Freedom of Information Act[14] as authority for keeping files secret from the individual as well as from Congress. They then turn around and cite "inherent power"[15] or "housekeeping authority"[16] as a reason for maintaining data banks and computerized files on certain individuals; or they may cite the conclusions of independent Presidential factfinding commissions.[17]

---

10. Department of Transportation response. Testimony of Secretary Volpe. *Id.* at 720. Many other agencies will inform the individual of the general contents of his file, if he is denied some right, benefit or privilege and regulations permit a hearing or right of confrontation or cross-examination—but not before.

11. Department of Health, Education and Welfare, series of letters over a two year period on file with Subcommittee, and as of March, 1972, no response has been received containing substantive answers.

12. Directive, ICGP-G-S3, Jan. 9, 1971, *Release of Official Information to Legislative Branch of Government. 1971 Hearings*, at 1179.

13. Ervin, *Secrecy in a Free Society*, 213 NATION 454 (1971). *See generally Hearings on Executive Privilege Before the Subcomm. on Separation of Powers of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. (1971). Testimony by Senator Tunney at 381 and William Rehnquist at 420.

14. 5 U.S.C. § 552 (1970).

15. *See, e.g., 1971 Hearings*, at 375, 431, 385. Testimony of Assistant Secretary of Defense Froehlke. *Id.* at 602, 599; testimony of Assistant Attorney General Rehnquist, note 13, *supra.*

16. *See, e.g.*, Justice Department response to Subcommittee questionnaire.

17. For Defense Department reliance on the findings of the National Advisory Commission on Civil Disorders (Kerner Commission), see testimony of Assistant Secretary of Defense

So far the survey results show a very wide-ranging use of such technology to process and store the information and to exchange it with other federal agencies, with state and local governments and, sometimes, with private agencies.

Most of this is done in connection with administration of Government's service programs. However, a number of these data banks and information programs may partake of the nature of large-scale blacklists. This is so because they may encompass masses of irrelevant, outdated or even incorrect investigative information based on personalities, behavior and beliefs. Unwisely applied or loosely supervised, they can operate to deprive a person of some basic right.

For instance, a Federal Communications Commission response[18] shows that the FCC uses computers to aid it in keeping track of political broadcast time, in monitoring and assigning spectrums, and in helping it make prompt checks on people who apply for licenses. The Commission reported that it also maintains a Check List, which now has about 10,900 names. This Check List, in the form of a computer print-out, is circulated to the various Bureaus within the Commission. It contains the names and addresses of organizations and individuals whose qualifications are believed to require close examination in the event they apply for a license. A name may be put on the list by Commission personnel for a variety of reasons, such as a refusal to pay an outstanding forfeiture, unlicensed operation, license

---

Froehlke, *1971 Hearings*, at 379; noting the Commission's finding that the "absence of accurate information, both before and during disorder, has created special control problems for police," and the recommendation that "Federal-State planning should ensure that Federal troops are prepared to provide aid to cities . . . ."

The Department also cited a report filed by Cyrus Vance following the Detroit 1967 disturbances. *1971 Hearings*, at 378.

For law enforcement reliance on the Kerner Commission and similar commissions, *see e.g.*, testimony of Richard Velde for the *Law Enforcement Assistance Administration. 1971, Hearings* at 608:

> Several States are also developing with LEAA funds information systems related to civil disorders. Most of these systems have as their objective either tension detection and forecasting or providing support to tactical units. It should be noted that the Kerner Commission studied this problem carefully and recommended that the police develop adequate intelligence for tension-detecting as well as one-the-scene information for tactical units. Many of the systems LEAA supports in the civil disorders area arose out of the recommendations of the Kerner Commission and similar commissions established by the States.

For reliance on Warren Commission finding of information gaps, *see* response to Subcommittee questionnaries by the Secret Service, Nov. 21, 1969, reprinted at 115 CONG. REC. 39,114 (1969), and by the State Department Jan. 4 and Mar. 10, 1970; both responses in Subcommittee file.

18. Response to questionnaire, in Subcommittee files, Mar. 25, 1971.

suspension, the issuance of a bad check to the Commission or stopping payment on a fee check after failing a Commission examination.

In addition, this list incorporates the names and addresses of individuals and organizations appearing in several lists prepared by the Department of Justice, other Government agencies, and Congressional committees. For example, the list contains information from the "FBI Withhold List," which contains the names of individuals or organizations which are allegedly subversive, and from the Department of Justice's "Organized Crime and Racketeering List," which contains the names of individuals who are or have been subjects of investigation in connection with activities identified with organized crime. Also included in the list are names obtained from other Government sources, such as the Internal Revenue Service, the Central Intelligence Agency, and the House Committee on Internal Security. According to the Commission, the use of the data arose in 1964 because during the course of Senate Hearings chaired by Senator McClellan, it was discovered that a reputed racketeering boss in New Orleans, Louisiana, held a Commission license. In order that such licensing not take place in the future, the Commission established liaison with the responsible divisions within the Department of Justice to be kept current on persons who might have such affiliations.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2,120,000 index cards.[19] According to the Commission, these bear lead information relating to possible questions of suitability involving loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of Congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II.

The Commission chairman reported:

> Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting.

---

19. *Id.* Aug. 18, 1970.

In another "security investigations index" the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigations made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

Then, the Commission keeps an "investigative file" of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

The Housing and Urban Development Department is considering automation of a departmental system which would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File.[20] A data bank consisting of approximately 325,000 3x5 index cards has been prepared covering any individual or firm which was the subject of, or mentioned prominently in, any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well.

In the area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs terminals throughout the country.[21]

According to the Secretary of the Treasury:

> These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and usable form. With the coordinated efforts of the Agency Service's intelligence activities, steady growth of the suspect files is expected.

There is the "Lookout File" of the Passport Office and the Bureau of Security and Consular Affairs.[22] This computerized file illustrates the "good neighbor" policy agencies observe by exchanging information in order to keep individuals under surveillance for intelligence and law enforcement purposes. Maintained apart from the

20. *Id.* June 22, 1970.
21. *Id.* May 28, 1970.
22. *Id.* Jan. 4, 1970.

twenty million other passport files, its basic purpose is to assist in screening passport applicants to make certain they are citizens of the United States and that they are eligible to receive passports. Requests for entry into this system are received from component agencies of the Department, from other government agencies, or in the limited category of child custody, from an interested parent or guardian.

The Department assured the Subcommittee that data recorded in this "Lookout File" is not disseminated. Rather, it serves as a "flag" which, if a "hit" or suspect is recorded, is furnished to the original source of the lookout and consists of the name of the individual and the fact that he has applied for a passport. The individual is not told that he is in the file until the information is used adversely against him. Then, according to the report, "he is fully informed and given an opportunity to explain or rebut the information on which the adverse action is based."

Among some of the reasons listed for people being in the Lookout File are the following:

> If the individual's actions do not reflect to the credit of U.S. abroad;
> If he is wanted by a law enforcement agency in connection with criminal activity;
> If a court order restricting travel is outstanding or the individual is involved in a custody or desertion case;
> If he is a known or suspected Communist or subversive;
> If he is on the Organized Crime and Rackets List or is a suspected delinquent in military obligations.

The Defense Industrial Security Clearance Office is preparing to computerize its card files on over one and a half million private citizens who are employees of businesses doing classified contract work for the Federal Government.[23]

The Federal Deposit Insurance Corporation maintains information on people now associated with banks insured by the FDIC or who have been associated with such banks in the past.[24] It keeps a file on the names of individuals gained from newspapers and other public sources if they are characterized as having an unsatisfactory relationship with any insured bank or any closed insured bank. This also includes information supplied to the Corporation by other inves-

---

23. *Id.* Aug. 1970. *See also 1971 Hearings*, at 375, Froehlke testimony on this and other Defense Department records systems.

24. Response to questionnaire, Feb. 22, 1972. *See also* 12 U.S.C. § 1811 *et seq.* (1964), Amendments to Federal Deposit Insurance Act, requiring bank recording and reporting to Internal Revenue Service transanctions, S. REP. 91-1139 and H.R. REP. 91-975.

tigative or regulatory agencies on persons connected with an insured bank.

The Army maintains the U.S. Army Investigative Records Repository (USAIRR) which contains about 7,000,000 files relating principally to security and criminal investigations of former and present members of the Army, civilian employees and employees of private contractors doing business with the Army. The other services maintain similar investigative files.[25]

There is a Defense Central Index of Investigation operated by the Army for the entire Defense Department. The Index is designed to locate any security or criminal investigative file for any Defense agency and will be computerized shortly. It contains identifying data such as name, date of birth and social security number on people who have ever been the subject of investigations.[26]

There are all the data banks and computers in the Department of Justice[27] for intelligence, for civil disturbance prevention; for "bad checks passers;" for organized crime surveillance; and for federal-state law enforcement cooperation through the computerized National Crime Information Center.

On the basis of our investigation of complaints reviewed by Congress,[28] I am convinced that people throughout the country are more fearful than ever before about those applications of computer technology and scientific information processing which may adversely affect their constitutional rights. Furthermore, my study of the Constitution convinces me that their fears are well founded.

First, they are concerned that through a computer error they may be denied basic fairness and due process of law with respect to benefits and privileges for which they have applied.

Secondly, they are concerned about illegal access and violation of confidentiality of personal information which is obtained about them by government or industry.

---

25. *See* note 23 *supra.*

26. Response to Subcommittee questionnaire, Aug. 1970. Also described in Froehlke testimony, note 23, *supra* and in Army Undersecretary Beal letter of Mar. 20, 1970, reprinted in *1971 Hearings, Part II* at 1051, and at 116 CONG. REC. 26327-51 (1970).

27. For descriptions and citations to supporting statutes and regulations, *see* response to Subcommittee questionnaires, *1971 Hearings, Part II* at 1312-68. *See also* discussion in testimony of Justice Department officials. *Id. Part I* at 597, 849.

28. For descriptions and summaries of some of these complaints and concerns, Remarks of Senator Ervin, 116 CONG. REC. 30,797, 41,751, 43,944 and 117 CONG. REC. S. 985 (daily ed. Feb. 8, 1971). In particular, note opening statements by Subcommittee Chairman each day of *1971 Hearings* outlining issues of concern for the day. Of interest here is a Dec., 1971 report, *A National Survey of the Public's Attitudes Toward Computers,* sponsored by the American Federation of Information Processing Societies and TIME MAGAZINE noting that:

These are actions which for any one individual or for entire groups may lead to a loss of the ability to exercise that "pursuit of happiness" which the Declaration of Independence declares is one of the unalienable rights of man.

These are actions which, by producing erroneous reports, may limit or deny a person's economic prospects and thereby impair that liberty which under the 5th and 14th amendments government may not impair without due process of law.

Arrest Records

This possibility is illustrated by a letter[29] I received from a man who describes the effect on his life of an incident which occurred when he was fifteen years of age. In connection with a locker theft, he was taken to the police station, finger-printed, questioned, and then he left, cleared of charges. He was not involved in any incident subsequently except a few minor traffic violations. He served 11 years in the armed services and held the highest security clearances. After gaining employment with a city government, he discovered that the youthful incident was, 15 years later, part of an FBI file and distributed to employers on request. He was asked to explain the incident for personnel records and to state why he withheld the information. Although he was unaware of the record, he believes the failure to list the incident was a factor in not gaining employment in several instances, and he was told he would have to institute court action to have the record expunged.

The problem he and millions of others face with respect to their records is illustrated by a regulation issued by the Attorney General last year restating the goal of the Federal Bureau of Investigation "to conduct the acquisition, collection, exchange, classification, and preservation of identification records . . . on a mutually beneficial

---

There is major concern about the use of large computerized information files. Thirty-eight percent of those surveyed believe computers represent a real threat to people's privacy as opposed to fifty-four percent who disagreed. Sixty-two percent are concerned that some large organizations keep information about millions of people. In addition, fifty-three percent believe computerized information files might be used to destroy individual freedoms; fifty-eight percent feel computers will be used in the future to keep people under surveillance; and forty-two percent believe there is no way to find out if information about you stored in a computer is accurate. In general, the public believes government should make increased usage of computers in a number of areas, that such usage will make government more effective, and that there will, and should be, increasing governmental involvement in the way computers are used.

29. Letter, identity withheld, in Subcommittee files with comment by the Director of the Federal Bureau of Investigation.

basis."[30] Among the agencies listed as eligible to receive and supply information were railroad police, banking institutions and insurance companies.

In Washington, D.C., a young man who was an innocent bystander during a campus demonstration was arrested by police and then released. Knowing that the FBI could distribute such records to employers, he hired a lawyer and spent large sums of money in a suit to have his arrest record expunged. The lower court denied his request, but the Court of Appeals ruled that, in the District of Columbia at least, arrest records should be expunged for innocent bystanders caught up in mass police arrests.[31]

In another case, a young man was arrested on probable cause and fingerprinted in California. When the police could not connect him with the case, he was released. He sought to have his arrest record expunged, or alternatively, to have strict limitations placed on its dissemination to prospective employers and others by the Federal Bureau of Investigation. While the U.S. District Court denied his request for expungement, it did say that his arrest record may not be revealed to prospective employers except in the case of any Federal agency when he seeks employment with that agency. However, it could be distributed for law enforcement purposes. Congress later restored this power to the F B I temporarily in an annual appropriation bill.

Judge Gesell's comments in this case of *Menard* v. *Mitchell*[32] are significant for the issue of arrest records, but also for the Army's computer surveillance program and for many other government in-

---

30. 28 C.F.R. § 0.85 (b); codifying rulings by the Attorney General pursuant to 28 U.S.C. §534 which provides:

> (a) The Attorney General shall–
>
> (1) acquire, collect, classify, and preserve identification, crime and other records; and
> exchange these records with, and for the official use of, authorized officials of the Federal Government, the States cities, and penal and other institutions.
>
> (b) The exchange of records authorized by subsection (a) (2) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.
>
> (c) The Attorney General may appoint officials to perform the functions authorized by this section.

31. Morrow v. District of Columbia, 417 F.2d 728 (D.C. Cir. 1969). For a summary of case law on this subject, *see* Longton, *Maintenance and Dissemination of Records of Arrest Versus the Right to Privacy*, 17 WAYNE L. REV. 995 (1971).

32. Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970), *decision upon remand*, 328 F. Supp. 718 (D.D.C. 1971). The Court construed 28 U.S.C. § 534 narrowly to avoid the constitutional issues raised by *Menard* and found that:

telligence systems now being designed. He stated that while "conduct against the state may properly subject an individual to limitations upon his future freedom within tolerant limits, accusations not proven, charges made without supporting evidence when tested by the judicial process, ancient or juvenile transgressions long since expiated by responsible conduct, should not be indiscriminately broadcast under governmental auspices." He also said:

> The increasing complexity of our society and technological advances which facilitate massive accumulation and ready regurgitation of farflung data have presented more problems in this area, certainly problems not contemplated by the framers of the Constitution. These developments emphasize a pressing need to preserve and to redefine aspects of the right of privacy to insure the basic freedoms guaranteed by this democracy.
>
> A heavy burden is placed on all branches of Government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy. Systematic recordation and dissemination of information about individual citizens in a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move about in this land. If information available to Government is misused to publicize past incidents in the lives of its citizens the pressures for conformity will be irresistible. Initiative and individuality can be suffocated and a resulting dullness of mind and conduct will become the norm. We

---

It is abundantly clear that Congress never intended to, or in fact did, authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks.

It found certain faults with the present system: (1) State and local agencies receive criminal record data for employment purposes whenever authorized by local enactment, and these vary state by state and locality by locality. (2) The Bureau cannot prevent improper dissemination and use of the material it supplies to hundreds of local agencies. There are no criminal or civil sanctions. Control of the data will be made more difficult and opportunities for improper use will increase with the development of centralized state information centers to be linked by computer to the Bureau. (3) The arrest record material is incomplete and hence often inaccurate, yet no procedure exists to enable individuals to obtain, correct or supplant the criminal record information used against them, nor indeed is there any assurance that the individual even knows his employment application is affected by an FBI fingerprint check.

The Court invited Congressional action, noting that:

> with the increasing availability of fingerprints, technological developments, and the enormous increase in population, the system is out of effective control. The Bureau needs legislative guidance and there must be a national policy developed in this area which will have built into it adequate sanctions and administrative safeguards.

> are far from having reached this condition today, but surely history teaches that inroads are most likely to occur during unsettled times like these where fear or the passions of the moment can lead to excesses.

There are many similar cases pending throughout the states. Present laws are not sufficient to assure that an individual will be judged on his merit and not by inaccurate arrest records distributed by a national law enforcement computer.[33]

Law Enforcement Intelligence Records

Such threats to privacy and liberty arise with special force in the area of intelligence records. The Subcommittee study reveals two serious problems which have acquired national urgency through the introduction of computer technology. First, the problem of safeguarding intelligence information from improper release by government it-

---

33. Congressional response to the District Court's invitation has taken several forms, among them, a bill, S. 2545, introduced, but not acted on, to authorize the Attorney General to exchange criminal record information with certain state and local agencies. Remarks by Senator Bible, S. 14558, 117 CONG. REC., (daily ed. Sept. 20, 1971); and an amendment to the Department of Justice Appropriation Act of 1972 temporarily restoring the power over arrest records limited by the *Menard* decision. 117 CONG. REC. S.20461 (daily ed. Dec. 3, 1971). House Judiciary Subcommittee No. 4 on Mar. 16 began hearings on H.R. 13315, a bill introduced by Rep. Edwards, "to provide for the dissemination and use of criminal arrest records in a manner that insures security and privacy."

A related, but more comprehensive bill, S.2546, was introduced by Senator Hruska on Sept. 20, 1971, 117 CONG. REC. (daily ed.) to insure the security and privacy of criminal justice information systems. This is termed the Attorney General's response to an amendment to the Omnibus Crime Control Act of 1970, 18 U.S.C. §§ 351, 1752, 2516, 3731 (1964), requiring the Law Enforcement Assistance Administration to submit legislative recommendations to promote the integrity and accuracy of criminal justice data collection. LEAA demonstrated a prototype computerized system for exchange of criminal history information with the states, a project known as SEARCH – System for Electronic Analysis and Retrieval of Criminal Histories. In Dec. 1970, Project SEARCH was turned over to the FBI for the development of an operation system to be part of the National Crime Information System. The bill deals with criminal offender record information as well as criminal intelligence information.

A discussion of the philosophical, constitutional and legal issues and problems related to such a computerized system is found, with bibliographies, in *Security and Privacy Consideration* in *Criminal History Information Systems, Technical Rept. No. 2,* July, 1970, by Project SEARCH, California Crime Technological Research Foundation, funded by the Law Enforcement Assistance Administration, Department of Justice. Also pertinent is the testimony of LEAA officials on the use of information and intelligence systems by criminal justice agencies. *1971 Hearings,* on the National Crime Information Center. *Id.* at 914.

For a model state act proposed for criminal offender record information, *See generally Technical Memorandum No. 3,* May, 1971 by Project SEARCH.

As we have a highly mobile population, so we have a highly mobile criminal population, which requires that governments be able to share rapidly the information in their data banks in the interest of law enforcement. The problem is determining what agencies and what officials should control what information.

self, and secondly, the problem of confining its collection to appropriate areas and subjects.

Government has, and should have, power to collect information, even raw, unverified intelligence information, in fields in which government has a lawful, legitimate interest. But this great power imposes a solemn responsibility to see that no one is given access to that information, except the Government itself for some legitimate purpose. There could never, for instance, be justification for Government to disclose intelligence gathered about citizens pursuant to its powers, to other citizens for their own personal or financial aggrandizement. Nor should Government through disclosure of confidential documents aid and abet the writing of sensational articles in private journals operated for commercial profit.

Nevertheless, the Subcommittee received testimony and evidence about two cases which illustrate the misuse of confidential intelligence information for such purposes.

One involved a man in political life, the mayor of San Francisco, who was the subject of an article in Look Magazine purporting to establish that he associated with persons involved in organized crime. When the Mayor sued the magazine for libel, he undertook through subpoena power to learn the basis for such charges and where and how the authors obtained their information. He learned that they had received confidential information and documents from intelligence data banks. The information came from files and computer printouts of a number of major Federal, state and local government law enforcement agencies. They involved the U.S. Attorney General's Office, the Federal Bureau of Investigation, Internal Revenue Service, Federal Bureau of Narcotics, the Customs Bureau, the Immigration and Naturalization Service, the California Criminal Identification and Investigation Bureau, the California State Department of Justice, and the Intelligence Unit of the Los Angeles Police Department. By their own testimony for the case, the authors of the article admitted that they examined, obtained or borrowed originals or copies of such law enforcement records containing much raw unevaluated intelligence information on numerous people including the names of three U.S. Presidents, the state Governor, a number of Senators, and many private law-abiding citizens, not accused of any crime. These documents were obtainable despite the fact that many of them were stamped "Confidential" or

> Property of U.S. Government For official use only. May not be disseminated or contents disclosed without permission . . .

There is more about these and other disclosures in the hearing record but I believe the Mayor's testimony[34] illustrates many of the dangers to privacy in this age of large investigative networks and instant computerized dossiers. It also illustrates the lack of sufficient criminal, civil, or administrative sanctions against unwarranted sharing and disclosure of such confidential information. To my knowledge, no punitive action was taken except for a disciplinary personnel action filed against an agent of the Federal Bureau of Investigation, who was then allowed to retire.

The weakness of any applicable regulations is demonstrated by the report of the Bureau of Narcotics and Dangerous Drugs that its current disclosure order "would not cover the release of collateral intelligence information, information contained in dead files, or information on nondefendants, such as that disclosed in the Alioto testimony." The Bureau further stated that under the provisions of its new Agents Manual it is only a "breach of integrity" to make unauthorized disclosure of files which are restricted to official use.[35]

Misuse of Military Intelligence Records

Another case[36] illustrates how the Army's investigative intelligence services and files were put to private use to obtain the dismissal

34. *See 1971 Hearings* at 493-530, Testimony of Joseph Alioto, Mayor of San Francisco, and exhibits submitted. For response of Justice Department officials, see testimony of William Rehnquist, *id.* at 604, 878-88, and a series of memoranda from the Federal Bureau of Investigation, the Bureau of Narcotics and Dangerous Drugs, which memoranda were submitted by Assistant Attorney General Rehnquist with the caveat that:

> Under the traditional notions of separation of powers, it seems to me probable that the Department could justifiably decline to furnish portions of this information . . . *Id.* at 1371.

35. *1971 Hearings,* Part II at 1375. In his memorandum of Mar. 5, 1971, the Director of the Bureau of Narcotics and Dangerous Drugs noted " . . . it is possible that the documents or information in these four exhibits could have been passed to the LOOK reporters by a BNDD employee." He cites BNDD Order 0-98, May 27, 1970 as the Bureau's current public information policy and as essentially a restatement of 28 C.F.R. Pt. 50, § 50.2, which covers the dissemination of most types of information for the Department. However, he states that the

> strongest applicable regulations in this matter are found in 28 C.F.R. Pt. 45, § 45.735: "No employee shall use for financial gain for himself or for another person, or make any other imporoper use of, whether by direct action on his part or by counsel, recommendation, or suggestion to another person, information which comes to the employee by reason of his status as a Department of Justice employee and which has not become part of the body of public information."
>
> Obviously, the disclosure of documents stamped "For official use only" would be contrary to this regulation if, in fact, the disclosures were made by Department of Justice employees.

36. For statement submitted by a Special Agent of Military Intelligence and related correspondence, *see 1971 Hearings,* Part II at 1451-1457.

of an employee of a private business. In this instance an Army intelligence agent whose routine duties involved security investigations and surveillance for the Army's civil disturbance prevention program described to the Subcommittee how he was ordered by his superiors to conduct an investigation of the bank loan records, police and court records of the private citizen and was told to give the resulting information to the employee's supervisor. He later learned that the investigation had been ordered by an intelligence officer as a personal favor for an official of the company. When the agent reported this to his superiors, he was told in a classified letter that the matter involved "national security." A year later, following his separation from the service, the agent reported the incident to the Inspector General of the Assistant Chief of Staff for the Pentagon, who began an investigation. All of his allegations were confirmed and firm disciplinary actions were taken against the guilty officers. It was too late, however, for the subject of the Army investigative report, who had already been dismissed.

These cases illustrate the concerns over political administrative and technical problems of access, confidentiality and purging of erroneous or outdated records in computer systems. But these are issues which have long concerned legislatures, bar associations and others.

The major reason for public apprehension about computer technology and information sciences is the use of them to acquire, process, analyze and store information about activities and matters which are protected by the First Amendment.

What people writing to Congress fear most is the uses to which this technology may be put by men of little understanding but great zeal. They know that, applied to unlawful or unwise programs, computers merely absorb the follies and foibles of misguided politically-minded administrators.

In Federal Government, the new technology, combined with extended Federal-state services and their spin-off information systems, have produced vast numbers of investigators, analysts, and programmers devoted to the study of people and society. With the zeal of dedicated civil servants, they are devoted to the building of data bases on the habits, attitudes and beliefs of law-abiding citizens. Much of what they gather is trivial; much of it goes far beyond the needs of government. Some of it is shared extensively and often unnecessarily by agencies who are components of these large information systems.

People seeking government jobs in some agencies are told to reply to personality tests asking:

I believe there is a God.

I believe in the second coming of Christ.
I believe in a life hereafter.
I am very religious (more than most people).
I go to church almost every week.
I am very strongly attracted by members of my own sex.
I love my father.
My sex life is satisfactory.
Once in a while I feel hate towards members of my family whom I usually love.
I wish I were not bothered by thoughts about sex.

When the Subcommittee held hearings on these practices, government officials explained that there was no right or wrong answer to the questions, that the responses were coded and analyzed by the computer.[37]

I asked whether they did not think such inquiries violated the privacy of the individual's thoughts about matters that were none of the business of government. The reply was that there was no Supreme Court decision holding that people who apply for federal employment have a constitutional right to privacy.

There was a Civil Service program telling employees to fill out computer punch cards stating their racial, ethnic or national origin along with their social security number.[38] In the land renowned for being the "melting pot" of the world, over 3 million individuals had to analyze their backgrounds and reduce them to one of four squares on an IBM card. If they protested that these matters were none of the business of government, they were blacklisted in their offices and harrassed with computer-produced orders to return the completed

---

37. *See generally Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the State Comm. on the Judiciary*, 89th Cong., 1st Sess. (1965) and *Hearings on S. 3779* on *Privacy and the Rights of Government Employees*, 89th Cong., 2d Sess. (1966).

38. *See 1966 Hearings, supra* note 37. In connection with a proposal introduced to protect the constitutional rights of employees of the executive branch and to prevent unwarranted governmental invasion of their privacy, *see* Senate remarks of Senator Ervin including discussion of need for law prohibiting requirements to reveal information on race, religion, national origin, personal family relationships, sexual attitudes and conduct and religious beliefs and practices in 112 CONG. REC. 16081, 18634 (1966), 113 CONG. REC. 4039, 10663, 27994 (1967), 114 CONG. REC. 11235, 17161, 19613 (1968), 115 CONG. REC. 2343, 117 CONG. REC. (daily ed. Apr. 1 and May 11, 1971). By such legislation, government may be prevented from intruding into protected First Amendment areas on subjects which should have nothing to do with the operation of a civil service merit system. By exclusion of such sensitive, subjective information from the computer systems, initially, government will be precluded from basing individual or general social judgments on outdated standards, changing mores, variants in ethnic, cultural or geographical backgrounds, or previous conditions of the individual's mind, heart, and personality. It will necessarily be confined to a consideration of current information relevant and pertinent to the problem at hand.

questionnaire. The resemblances between this program and those of totalitarian governments in our recent history were all too obvious.

The Census Bureau makes more use of computer technology for personal inquiries than anyone.[39] It conducts surveys for its own uses backed by the criminal and civil sanctions. One of these, the decennial census, asked people such questions as:

> Marital Status: Now married, divorced, widowed, separated, never married.
> (If a woman) How many babies have you ever had, not counting stillbirths?
> Do you have a flush toilet?
> Have you been married more than once?
> Did your first marriage end because of death of wife or husband?
> What was your major activity 5 years ago?
> What is your rent?
> What is your monthly electric bill?
> Did you work at any time last week?
> Do you have a dishwasher? Built-in or portable?
> How did you get to work last week? (Driver, private auto; passenger, private auto; subway; bus; taxi; walked only; other means).
> How many bedrooms do you have?
> Do you have a health condition or disability which limits the amount of work you can do at a job?
> How long have you had this condition or disability?

Under even heavier sanctions, the Census Bureau puts questionnaires to farmers, lawyers, owners of businesses, and others, selected at random, about the way they handle their business and finances.[40]

---

39. *See generally Hearings on S.1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Committee*, 91st Cong., 1st Sess. (1969) and hundreds of letters and complaints about coercive statistical questionnaires. Appendix also contains judicial, legal and constitutional research materials as well as examples of many social and economic questionnaires. *See also* Pipe and Russell, *Privacy: Establishing Restrictions on Government Inquiry*, 18 AMER. UNIV. L. REV. 516 (1969). For a summary of the hearings, *see* Senate remarks of Senator Ervin, 115 CONG. REC. 17718 (1969). For possible political uses of such information acquired as economic and social indicators, *see* Report by House Government Operations Committee, Subcommittee on Government Information, on Department of Labor briefings on economic statistics; and 23 WESTERN POL. Q. 235 (1970). *See also* the finding and recommendations on privacy and confidentiality of the PRESIDENT'S COMMISSION ON FEDERAL STATISTICS (1971).

40. *See 1969 Hearings, supra* note 39,. testimony on behalf of the National Federation of Independent Business at 199, of attorney and farm owner William Van Tillburg at 74, W. Schliestett, businessman at 66, J. Cannon, attorney at 7,263.

The Census Bureau also makes surveys for many other departments and agencies.[41] For example, they put out statistical questionnaires which the Department of Health, Education and Welfare wanted to send to retired people asking:

— How often they call their parents;
— What they spend on presents for grandchildren;
— How many newspapers and magazines they buy a month;
— If they wear artificial dentures;
— "Taking things all together, would you say you're very happy, pretty happy, or not too happy these days?"
— And many other questions about things on which govern- has no business demanding answers.

These people are not told that their answers are voluntary, but are harrassed to reply and are given the impression they will be penalized if they do not answer.[42]

There are many other examples of inquiring social and economic data that are backed by the psychological, economic, or penal sanction of government. Clearly, Government has great need for all kinds of information about people in order to govern efficiently and administer the laws well; similarly, Congress must have large amounts of meaningful information in order to legislate wisely.

However, I believe these examples of governmental data collection illustrate my contention that the First Amendment wraps up the principle of free speech, which includes the right to speak one's thoughts and opinions as well as the right to be free of governmental coercion to speak them.

There are other examples of government programs which, well-meaning in purpose, are fraught with danger for the very freedoms which were designed to make the minds and spirits of all Americans

41. *Id.* at 830. Table of Census surveys of population and households, conducted for other government agencies, with indication of penalties and compliance techniques. In many of these, the data is kept on tape or film by both the Census Bureau and the sponsoring agency, and the confidentiality rules of the sponsoring agency apply.

42. *Id.* at 251. Assistant Secretary of Commerce Chartener:

> Assistant Secretary of Commerce Chartener: The wording deliberately has been rather subtle in its form. We never use the word "mandatory" on a questionnaire. Instead, people will be told that "your answer is required by law." In other cases, they may be told that a survey is authorized by law or it is important to your government or something of that sort. Now, the followup procedure is used not for purposes of coercion but rather in order to verify the correctness of an address.
>
> Senator Ervin: Do you not agree with me that such a procedure is designed to implant in the mind of the recipient of these questionnaires the impression that he is required by law to answer them?

free, and which work to keep America a free society. A number of these would be impractical, if not impossible, without the assistance computer technology and scientific data processing.

It is those First Amendment freedoms which are the most precious rights conferred upon us by our Constitution: the freedom to assemble peaceably with others and petition government for a redress of grievances; the freedom to worship according to the dictates of one's own conscience free of government note-taking; the freedom to think one's own thoughts regardless of whether they are pleasing to government or not; the freedom to speak what one believes whether his speech is pleasing to the government or not; the freedom to associate with others of like mind to further ideas or policies which one believes beneficial to our country, whether such association is pleasing to government or not.

The Secret Service

In the pursuit of its programs to protect high government officials from harm and federal buildings from damage,[43] the Secret

---

Mr. Chartener: If it is a mandatory questionnaire that would be the case. In other instances, the repeated mailings which may go up to five or may involve telephone calls or even a personal call are simply a means of emphasizing the importance that the Government feels in getting this response . . . .

The Department of Commerce opposed enactment of a simply-worded statute advising people that their responses to these statistical questionnaires were voluntary. *Id.* at 262.

Senator Ervin: Would the Department of Commerce and its Bureau of the Census be opposed to enactment of Federal statutes which would require that the Bureau of the Census advise every citizen on a questionnaire sent out by the Bureau that where it is not required by law, not mandatory, this is an effort to elicit information desired by the Government on a voluntary basis?

Mr. Chartener: Senator, I think we would oppose that. This is a matter of rather subtle psychology. I do not think, personally, and this is the position of the Department, that we ought to go out of our way to tell people they do not need to bother filling out this questionnaire . . . .

Senator Ervin: You think the statutes governing those questionnaires, which are mandatory and which are subject to the criminal penalty if not answered readily, are understandable by the average layman?

Mr. Chartener: I do not think any law is written to be readily understandable by the average layman. That is why we have lawyers.

But compare the testimony of the Secretary of the Department of Health, Education and Welfare in the *1971 Hearings* at 788, opposing legislation, but favoring administrative notice of voluntariness for that Department's forms.

43. 115 CONG. REC. 3356 (1969) and guidelines printed there. *See also* note 17, *supra,* correspondence and guidelines printed at 1541, *1971 Hearings,* Part II. *See* remarks of

Service has been pressured to create a computerized data bank. Their guidelines for inclusion of citizens in this data bank requested much legitimate information but also called for information on "professional gate crashers;" "civil disturbances;" "anti-American or anti-U.S. Government demonstrations in the United States or overseas;" pertaining to a threat, plan, or attempt by an individual or group to "embarrass persons protected by the Secret Service or any other high U.S. Government official at home or abroad;" "persons who insist upon personally contacting high government officials for the purpose of redress of imaginary grievances;" and "information on any person who makes oral or written statements about high government officials in the following categories: (1) threatening statements, (2) irrational statements, and (3) abusive statements."

Americans have always been proud of their First Amendment freedoms which enable them to speak their minds about the shortcomings of their elected officials. As one in political life, I have myself received letters I considered abusive. Similarly, I have uttered words which others have deemed abusive. While I am not a "professional gate crasher," I am a malcontent on many issues. I have written the President and other high government officials complaining of grievances which some may consider imaginary; and on occasion, I may also have "embarrassed" high government officials.

One man wrote me his concern about this program and commented:

> The Secret Service ought to go after my mother-in-law, too. On her last visit she said that the Vice President doesn't seem to have too many brains. She also said that Senator ..... has a face like a carbuncle. Should I report this to the Secret Service?[44]

There is no doubt that the physical protection of the President and high government officials is a legitimate government purpose and all reasonable means must be taken in pursuit of it. Nevertheless, such broad and vaguely worded standards for investigating and adversely reporting Americans to their government on the basis of their utterances could, at one time or another, include most members of Congress and most politically aware citizens. It could cover heated words exchanged in political debate and discussion anywhere in the country. Yet civil and military officials throughout the Federal

---

Rep. Stanton, 118 CONG. REC. at H208 (daily ed. Jan. 24, 1972) [Complaints Against Secret Service].

44. Letter in Subcommittee files.

government and in some local law enforcement agencies were requested to report people coming to their attention who were thought to fit these criteria.

The Subcommittee has not received complete answers to our questionnaire on the subject of this computer and the national reporting system it serves. However, we have indications that other broad and zealous information programs, including the Army civil disturbance system,[45] are sharing or feeding on entries which, if not carefully evaluated, may produce serious consequences for the rights and privileges of citizens. Illustrating the misunderstandings and misinterpretations possible is the fact that military doctors have expressed to me their concern about an allegedly "secret" agreement between the Defense Department and the Secret Service which they were told was a recent one and which required reporting of all servicemen receiving administrative discharges. One psychiatrist writes of his concern for the confidentiality of medical records in such action:

> I see very little reason for this. My impression of the individuals whom I recommended for such a discharge was that these were immature individuals who were not able to adapt to the service for one reason or another. Not by any stretch of the imagination were these individuals unpatriotic or a threat to the security of the nation.[46]

When I asked the Secretary of the Navy about this, the Subcommittee was informed that a person is not reported to the Secret Service merely because he received an administrative discharge from the Navy or Marine Corps.[47] However, we were informed that Pursuant to Naval regulations issued under a secret 1965 Agreement,[48]

---

45. *See Department of the Army Civil Disturbance Information Collection Plan*, May 2, 1969, collection priorities and requirements and distribution list for government agencies. Printed in *1971 Hearings* at 1126, 1136. This plan also appears with remarks of Senator Bayh, 117 CONG. REC. 2290 (daily ed., Mar. 2, 1971).

46. Letters in Subcommittee files (identities withheld).

47. Letter of inquiry from Subcommittee Chairman, July 6, 1971, citing the large number of reasons for which a person can receive an administrative discharge, ranging from family hardship to national security grounds, the inadequate procedures and safeguards surrounding such discharges, and the threat to individual freedom from unrestricted reporting of law-abiding citizens, who may become subjects of official surveillance through no fault of their own or of the Secret Service.

48. This December 14, 1965 agreement between the Defense Department and the Secret Service was implemented within the Navy Department by SECNAV Instruction 5500.27, 18 March 1966, which contains a copy of the agreement. Administrative authority for this regulation is cited as Defense Dept. Directive 5030.34, dated 30 Dec. 1965; statutory authority for assistance to the Secret Service is cited as P.L. No. 90-331 (June 6, 1968) which provides for assistance to the Secret Service on request.

the Navy reports an average of 400 persons annually. We learned, for example, that among the many categories of people to be reported were not only servicemen but civilian employees of the Defense Department who were discharged on security or suitability grounds and who showed "evidence of emotional instability or irrational or suicidal behavior, expressed strong or violent sentiments against the United States," or who had "previous arrests, convictions, conduct or statements indicating a propensity for violence and antipathy for good order in Government."[49]

Military Spying

Another example of First Amendment information programs is the Army program for spying on Americans who exercised their First Amendment rights. Despite these rights, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.[50]

Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, tape-recorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

---

49. Appendix B of Agreement. Under Appendix A, identification data, photograph, physical description, date and place of birth, employment, marital status and identifying numbers are to be furnished, together with summaries or excerpts from DOD files as applicable to an individual or group reported.

In a related exchange of correspondence, the Subcommittee Chairman, in response to complaints, directed an inquiry to the Secretary of the Navy, on April 22, 1970 about a Navy directive which required that in any case where enlisted personnel were to be separated under other than honorable conditions within the continental United States, local civil police authorities were to be notified in advance of the name, race, sex and place and date of birth of the person, and of the time and place such separation is to be effected. This regulation seemed to serve no useful function since the Army and the Air Force functioned without one. On May 7, 1970, the Navy Department notified the Subcommittee that they concurred in this view and would delete the reporting requirement. (Correspondence in Subcommittee files.)

50. For legal and constitutional implications, as well as a comprehensive historical account, *see* testimony of Christopher Pyle, an attorney and former Captain in Army Intelligence. *See 1971 Hearings* at 147, and exhibits providing examples of nation-wide military surveillance.

With very few, if any, directives[51] to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.[52]

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.[53]

The Army attempts to justify its surveillance of civilians by asserting that it was collecting information to enable the President to predict when and where civilians might engage in domestic violence, and that the President was empowered to assign this task to it by the statutes conferring upon him the power to use the armed forces to suppress domestic violence.

I challenge the validity of this assertion.

Under our system, the power to investigate to determine whether civilians are about to violate federal laws is committed to

---

51. *See* Ervin, *Privacy and Governmental Investigations*, 1971 UNIV. ILL. L. FORUM 137 (1971) for an account of the various plans and their lack of relevance to the problem of putting down civil disturbances, and for analysis of the Defense and Justice Department's claims to constitutionality for the actions of the military. Texts of four "Plans," *1971 Hearings* at 1123, 1119, 1154, 1731; Memorandum at 1139, 1141, 1278-98, showing attempts by civilians to cut back on the program.

52. The bulk of investigative activity by the Army's own personnel occurred at the field level. Agents collected information and filed "spot reports," "agents reports," and "summaries of investigation." Most of this data was forwarded up the chain of command but record copies were kept in data centers at every level of command. Manual files were maintained at every level. At least four and possibly more computer systems were employed to store, analyse and retrieve the information collected. Many files on lawful citizens were microfilmed and integrated with other files on persons who were suspected of violations of security and espionage laws. These computer systems were located in the headquarters of the Intelligence Command (Fort Holabird), the Continental Army (Fort Monroe), the Third Army Corps (Fort Hood), and in the Pentagon. More than one computer data bank was maintained in some of these locations. (Subcommittee investigation).

53. Testimony of Ralph Stein on the difficulty of labeling young people on the basis of their speech, when a difference of one digit was the difference between a communist and a non-communist. *1971 Hearings* at 248, 260.

federal civil agencies, such as the FBI; and the power to investigate to determine whether civilians are about to violate state laws is reposed in state law enforcement officers.

If President Johnson believed he ought to have had information to enable him to predict when and where civilians might engage in future domestic violence, he ought to have called upon the FBI or appropriate state law enforcement officers for the information.

He had no power to convert the Army into a detective force and require it to spy on civilians.

This conclusion is made plain by the Constitution and every act of Congress relating to the subject. Sections 331, 332, 333 and 334 of Title 10 of the United States Code certainly did not confer any such power on the President. These statutes merely authorized him to use the armed forces to suppress domestic violence of the high degree specified in them, and conditioned their use for that purpose upon his issuing a proclamation immediately ordering the offenders "to disperse and retire peaceably to their abodes within a limited time."

The only other statute relevant to the subject is section 1385 of Title 18 of the Code, which prohibits the use of any part of the Army or Air Force "as a possee comitatus or otherwise to execute the law . . . except in cases and under circumstances expressly authorized by the Constitution or Act of Congress."

The legislative history of this statute is fully revealed in the opinion of United States District Judge Dooling in *Wrynn v. United States*, 200 F. Supp. 457 (E.D.N.Y. 1961). When the words of this statute are read in the light of its legislative history, it is obvious that the statute is not limited by the expression "as a posse comitatus or otherwise," but operates as a prohibition against the use of the Army to execute the laws without reference to whether it is employed as a posse comitatus or as a portion of the Army. Indeed, the statute embodies "the inherited antipathy of the American to the use of troops for civil purposes." [200 F. Supp. at 465].

President Johnson's use of the troops to spy on civilians, to build data banks and create computerized information systems, discloses that relevance of this statute to our day is sadly clear. Since neither the Constitution nor any Act of Congress expressly, or impliedly, authorized such use, the President was forbidden by section 1385 of Title 18 of the United States Code to use the Army to spy on civilians.

The Army's spying violated First Amendment freedoms of the civilians who became aware that they or the groups to which they belonged had been placed under surveillance. This is so because it

undoubtedly stifled their willingness to exercise their freedom of speech, association and assembly.[54]

If any proof were needed of the logic and truth of this statement, it can be drawn from such testimony as the Subcommittee received from Dr. Jerome Wiesner who commented,

> Many, many students are afraid to participate in political activities of various kinds which might attract them because of their concern about the consequences of having a record of such activities in a central file. They fear that at some future date, it might possibly cost them a job or at least make their clearance for a job more difficult to obtain.[55]

The Subcommittee has heard no testimony yet that the Army's information program was useful to anyone. The only result of the

---

54. *See* Brief for Respondents filed in Tatum v. Laird in the Supreme Court of the United States, No. 71-288, challenging the Army's surveillance program, and arguing that plaintiffs' claims are justiciable and ripe for adjudication; that the present inhibiting effect on the exercise of First Amendment rights creates a justiciable controversy; that the justiciability of their claims is enhanced because the military exceeded its constitutional and statutory authority and intruded into civilian affairs; that they have standing to adjudicate these claims for themselves and the claims of others similarly situated; and finally, that they argue that their case cannot be mooted by the Army's assertion that its domestic surveillance activity has been reduced. The appendix contains an interesting and landmark study of the chilling effect of overbroad governmental programs on First Amendment activity from the social science view.

All of the plaintiffs named have been subjects of political surveillance, and all are believed to be subjects of reports, files, or dossiers maintained by the Army.

In an amici brief filed by Senator Ervin on behalf of the Unitarian Universalist Association, the Council for Christian Social Action, United Church of Christ, the American Friends Service Committee and the National Council of Churches of Christ, the question posed for review is framed as follows:

> Do individuals and organizations not affiliated with the armed services present a justiciable issue under the First, Fourth, Fifth and Ninth Amendments when they allege that their rights of free expression, privacy and association have been infringed by unauthorized, unnecessary and indiscriminate military investigation of their political activities and personal lives? Brief for Respondents as amicus curiae at 7, Laird v. Tatum, No. 71-288 (1971).

> Essential though the freedoms are, they are not easily exercised in a climate of fear, discord, and dissension, especially when the ideas being expressed are those which are displeasing to government and unsettling to the majority of citizens . . . . It is as such a time that the First Amendment is most necessary, most in danger, and most difficult to exercise . . . . The First Amendment however, was made for the timid as well as for the brave. While government cannot instill courage in the meek, it may not take advantage of a climate of fear to undertake a program which has the effect of restricting the First Amendment only to the very courageous. Government action, such as military surveillance, seemingly innocuous in the abstract, has the very real effect of suppressing the exercise of the First Amendment. The coercive power of this government action lies in the national climate of fear and doubt, and in the very real, tangible apprehension of some unknown form of retribution by government on those who it fears and therefore watches. That such apprehension exists in America today is manifest. *Id.* at 15.

testimony by the Defense Department was to confirm my belief that under the Constitution and under the laws, the Army had no business engaging in such data-gathering and that the scope and breadth of the surveillance was so broad as to be irrelevant to the purpose.

Congress has still to discover the complete truth about these Army computers. Apparently, even officials responsible for intelligence did not know of the existence of the computers for implementing the program. The Subcommittee has repeatedly requested the testimony of the Army Generals who would be most knowledgeable about the computers and what they contained. We have just as repeatedly been denied their testimony as well as delivery and declassification of pertinent documents demonstrating the scope and purpose of the program.[56] The Army said it would cut back on the data-gathering on lawabiding citizens and would defer to the Department of Justice. So I asked the Justice Department officials how many computers that Department had containing information on people who lawfully exercised their First Amendment freedoms.[57]

I had seen newspaper articles quoting the director of the Justice Department's Interdivisional Information Unit. He said there that the computer's list of thousands of names is not a register of "good guys" or "bad guys." "It is simply a list of who participated in demonstrations, rallies and the like." This would include non-violent people as well as violent, he said.[58] On the basis of these reports, I asked for the testimony of this official, but for some strange reason, he could not be located.

Despite questioning during the hearings and correspondence with the Justice Department, we have been unable to obtain an accurate description of the use of Justice Department computers for collecting, processing and analyzing information on lawful First Amendment activities of citizens. Nor have we been able to ascertain or obtain the standards followed by the Department in deciding what individuals should be the subjects in such files, or how they should be excluded from such files.

Legislative Remedies

There has been much discussion of the need for new laws granting access to individual records. I believe a person should have the

---

55. *1971 Hearings* at 765.

56. *See* exchange of correspondence on this subject. *Id.* Part II at 1046 A, 1180 Indices to letters.

57. *Id.* at 597, 849.

58. *Id.* at 616-22.

chance to expunge, update and correct his records. With the advent of systematic record-keeping, a man needs the chance which a businessman has to go into economic bankruptcy and obtain a discharge from his past.

I believe, however, that we must go beyond that relationship between the individual and his records. We must act to restore a healthy balance to the relationship between the citizen and his government, and necessarily between Congress and the Executive Branch. Mere access to and knowledge of his individual file is not enough. Remedial action must be addressed to the curbing of the power of government over the individual and to restricting its power to deny information about government programs. The claim to an inherent power to monitor, investigate and compile dossiers on law-abiding citizens on the off-chance that they might need to be investigated for a legitimate governmental purpose at some time in the future must also be opposed.

As a result of the Subcommittee's experience in playing hide-and-go-seek with the Federal Government's computers and with the people who plan and supervise them, I am convinced these computers have too much privacy today. The Congress, the press and the public should have available an *habeas corpus* action for entire computer systems and programs themselves. No department should be able to hide such broad-based data programs and information systems. If they are lawful, the American people then have a right to full knowledge about the operation of their government. If they are not lawful and relevant for some purpose, they should be exposed for what they are—attempts to intimidate citizens into silence and conformity.

First, we need to devise some judicial remedy for confronting and testing the nature, purpose, legality and constitutionality of governmental data banks and large-scale intelligence information systems which by their very existence may threaten the quality of our First Amendment freedoms or whose contents may affect economic prospects, reputations or rights. Now pending before the United States Supreme Court is just such a challenge to the Army surveillance program and the military data banks, including at least four computer systems for storing and processing information on American across the land. [*Tatum v. Laird*, no. 71-288 (1971) (argued March 27, 1972)] The lower court has denied standing to sue to plaintiffs who were subjects of surveillance and computer dossiers on grounds that they have not shown injury. [44 F.2d 947 (D.C. Cir. 1971)].

Congress must strengthen and enforce reporting requirements for computer systems. Not even in the audit of computers which the

present law requires the General Services Administration to conduct each year is it possible for Congress, the press, and the public to get minimum information about all of the management uses of computers in government.

Secondly, I believe we must devise legal means of assuring the reporting of large government data banks to a central office established independently of the executive branch. This would require the filing of policy statements describing exactly what agencies feed a particular information system and who would receive or access data routinely from a particular data bank. These policy statements should be public records. In this way, people would have due notice of possible sharing of information by other agencies or state or local governments.

Thirdly, out of these directives, a graphic national information-flow chart would be designed and made available for public inspection. An individual concerned about his record could then go to the respective agencies and exercise his rights under the Freedom of Information Law to inspect his files.

Fourth, there is a need to fully implement the principle of open government implicit in the Freedom of Information Law by reducing the number of exemptions in it which the Executive Branch may use to deny or withhold information. This would make the judicial remedies it contains more meaningful.

Fifth, I believe there must be established a new independent agency for setting and enforcing strict standards in software and hardware for the assurance of security, confidentiality and privacy of records. These would be applied to all phases of gathering, processing and transmitting information about people by government computer systems. This would include such problems as interception of electronic transmissions and tapping of systems.

Sixth, Congress must enact specific prohibitions on unconstitutional or unwise practices which unfairly augment government's power to invade individual privacy. Examples of such legislation would be: (1) a ban on use of military resources to conduct unwarranted surveillance over civilians and to create and share data banks on them, and (2) a ban on unconstitutional means of coercing citizens into revealing personal information about themselves.[59] Such a bill is S. 2156 which would prohibit requirements on applicants and employees to submit to lie detectors in order to work.[60] Another bill is S. 1438, designed to protect federal employees and applicants from

59. S.1791, 91st Cong., 1st Sess. (1969).
60. Senate remarks of Senator Ervin, 117 CONG. REC. (daily ed. June 24, 1971.)

unwarranted demands for information about such matters as their race, national origin, religious beliefs and practices, sexual attitudes and conduct, and personal family relationships.[61] Another necessary protection would be a prohibition on distribution of arrest records to private companies and severe restrictions on their availability within government.[62]

Seventh, is the need for America to take a stand on whether or not every person is to be numbered from cradle to grave, and if so whether or not that number is to be the social security number. Until now, the idea of a universal standard identifier has been merely discussed in philosophical terms, but the need to reduce people to digits for the computer age has prompted wide government use of the number for identifying individuals in government files. Private industries, businesses and organizations have followed suit to the dismay of many people who have registered strong complaints against this practice with the Subcommittee. They were supported by the findings of a Social Security Task Force which reported in 1971 that:

> The increasing universality of the Social Security Number in computer data collection and exchange presents both substantial benefits and potential dangers to society; and that in order to maximize the benefits and minimize the dangers, there needs to be developed a national policy on computer data exchange and personal identification in America, including a consideration of what safeguards are needed to protect individuals' rights of privacy and due process.[63]

In outlining the areas in which state legislatures and the Congress must make important judgments, this Task Force stated:

> Defining the proper role of the Social Security Number in society requires that broad social judgments be made first about the desirability of large-scale computer recordkeeping in various settings; second, about the kinds of data necessary and appropriate to record about individuals within a given setting; third, about the safeguards needed to insure that the computer is being used within a given setting in ways that protect fundamental human rights; and fourth,

---

61. See S. Rep. 92-554 for legislative history (Now pending before the House Post Office and Civil Service Committee with House versions).

62. *1971 Hearings* at 782 (complaints read into the hearing record by the Chairman).

63. SOCIAL SECURITY NUMBER TASK FORCE REPORT to the Commissioner 17 (May, 1971).

about the desirability of *any* kind of universal identification system in terms of its psychological impact on the individual citizen.[64]

Summary

From the Subcommittee study of privacy and government data banks one conclusion is undeniable. This is that the extensive use of computerized systems to classify and analyze men's thoughts, speech, attitudes, and lawful First Amendment behavior raises serious questions of denial of substantive due process to our entire society. To try to condense the truth about what men believe and why they believe is a futile exercise which can lead to that tyranny over the mind against which Thomas Jefferson swore eternal hostility. Without grave dangers to our constitutional system, we cannot permit government to reduce the realities of our political life and the healthy traffic in our marketplace of ideas to marks on magnetic tapes and data on a microfilm.

Professor Robert Boguslaw[65] eloquently described the dangers posed by this "technology-screened power" when he wrote that "the specification of future and current system states within this orientation characteristically requires an insistence upon a uniformity of

---

64. *Id.* at 15.

> It is clear that if the SSN became the single number around which all or most of an individual's interactions with society were structured, and if practices of the sort we have been discussing were to continue, the individual's opportunity to control the circumstances under which information about himself is collected and disclosed would be greatly circumscribed.

65. *See* BOGUSLAW, THE NEW UTOPIANS (1965), especially the chapter entitled *The Power of Systems and Systems of Power* at 181, 186, 190. I would dispute his observation of some years ago that people in the information-processing profession "are scientists and engineers—objective experts whose only concern is technical efficiency and scientific detachment." *Id.* at 198. It is indeed true, however, that:

> to the extent that customers (and this may include government agencies or private industry) abdicate their power prerogatives because of ignorance of the details of system operation, *de facto* system decisions are made by equipment manufacturers or information-processing specialists. *Id.* at 198.

Implicit in the various issues raised during the Subcommittee Hearings is the wise observation of Professor Boguslaw that:

> The paramount issues to be raised in connection with the design of our new computerized utopias are not technological—they are issues of values and the power through which these values become translated into action. *Id.* at 200.

In this case, I believe it is the constitutional value protected by the First Amendment.

perspective, a standardization of language, and a consensus of values that is characteristic of highly authoritarian social structures. Nonconforming perspectives, language, and values can be and, indeed, must be excluded as system elements."

He further points out certain engineering truths and certain human truths which face every politician, administrator, analyst and programmer who tries to use computers to convey either more or less than the straight facts about people. First is the truth that the strength of high-speed computers lies precisely in their capacity to process binary choice data rapidly. But to process these data, the world of reality must at some point in time be reduced to binary form. Second is the truth "that the range of possibilities is ultimately set by the circuitry of the computer, which places finite limits on alternatives for data storage and processing." Third is the truth "that the structure of the language used to communicate with the computer restricts alternatives." Then there is the truth "that the programmer himself, through the specific sets of data he uses in his solution to a programming problem and the specific techniques he uses for his solution, places a final set of restrictions on action alternatives available within a computer-based system."

It is in this sense that computer programmers, the designers of computer equipment, and the developers of computer languages possess power in our society.

These limitations of men as well as machines are what I remembered as I listened to the young Army analyst describing his assignment to condense truth for the Army data systems by assigning numbers to people on the basis of their speech and thoughts.[66]

On the shoulders of technology experts who are aware citizens rests the responsibility for guiding those politicians who seek computer-based solutions to political problems. At this point in our history, they, more than anyone, realize that computers have only those values which are designed and programmed into them.

If the attitude of the present Administration is any indication, Government will make increasing use of computer technology in pursuit of its current claim to an inherent power to investigate lawful activities and to label people on the basis of their thoughts. Municipal, state and federal agencies continue to plan, devise and build intelligence systems for many purposes. It devolves on those people involved in computer technology to make known the restrictions and the limitations of the machines as well as the alternatives for what is

---

66. *See* note 53 *supra.*

proposed. When the political managers ignore or abdicate their responsibility to assure the application of due process of law, they may have the final say over the constitutional uses of power.

What they say may not be popular with those who use their services, especially government departments. But I would suggest that when they advise on extending the power of government, they serve a higher law—the Constitution.

The technological forces which affect the quality of our freedoms come in many guises and under strange terminology. They are dreamers who would decry the advent of the computer as casting some sorcerer's shadow across an idyllic land. In their philosophical rejection or fear of this most intricate of machines, they would deny the spark of divinity which is the genius of man's mind; they would reject the progress of civilization itself. So there is no reason to condemn out of hand every governmental application of computers to the field of information processing or to systems study.

Our society has much to gain from computer technology. To assure against its political misuse, however, we need new laws restricting the power of government and implementing constitutional guarantees. We need increased political awareness of an independent nature by information specialists who understand the machines and the systems they constitute.

We do not, as some suggest, need new constitutional amendments to deal with these problems. The words of the original amendments will do, because they envelop our national concepts of personal freedom and I believe they can encompass anything which jeopardizes that freedom.

As Justice Oliver Wendell Holmes said:

> A word is not a crystal, transparent and unchanged; it is the skin of a living thought and may vary greatly in color and content according to the circumstances and the time in which it is used.[67]

I believe that Americans will have to work harder than ever before in our history so that the First Amendment remains a living thought in this computer age.

Otherwise, we may find the individual in our society represented not by a binary form, but by one digit.

And that will be "zero."

Otherwise, America may lose its cherished reputation as "the land of the Second Chance."

---

67. Towne v. Eisner, 245 U.S. 418, 425 (1918).

[*From the Yale Law Journal, Vol. 82, No. 7 (June 1973)*]

Privacy in the First Amendment

In the exercise of its traditional freedom, the press often discloses information about individuals which those individuals would rather conceal. When the information, though true, is particularly embarrassing or intimate, the person has sometimes felt sufficiently injured to sue the offending publisher—even though the publisher committed no physical intrusion, fraud or larceny to get the story. The claimed legal injury in such cases therefore consists only in having private information become public without the consent of the person whom the information concerns. When, in 1960, the late William Prosser sifted some 300 cases having to do with privacy,[1] he found that enough of these suits had been successful to constitute a common law cause of action.[2] Prosser named the action "the public disclosure tort" and listed it as one of four American common law torts which protect personal privacy.[3]

Even as Prosser identified the public disclosure tort action, he recognized that its existence might well interfere with the First Amendment right of the press to report on matters of legitimate public interest.[4] In the intervening decade the definition of what is "of legitimate public interest" has rapidly expanded under a series of Supreme Court decisions,[5] to the point where it is difficult to say confidently that any item of information which the press decides to publish is outside the

1. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).
2. For examples of such suits, see note 20 & p. 1470 *infra*.
3. Prosser, *supra* note 1, at 392-98.

Prosser did not attempt an exact definition of the public disclosure tort in his analysis. He described the tort generally as requiring that "something secret, secluded or private pertaining to the plaintiff" be invaded and that the something be publicized, but not requiring that the publication be false, or be for the commercial advantage of the defendant. *Id.* at 407. However, the examples he offered are mostly cases which do not fit neatly into the public disclosure category; the exception is Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931). *See* Prosser, *supra* note 1, at 392-98. Except for California, therefore, one finds it hard to say which states explicitly recognize the public disclosure tort. Most courts which uphold a "right to privacy" refuse to specify their rationale. Prosser himself ventures to identify only those states which recognize a privacy tort action in general, without breaking the recognized action down into his separate categories. *Id.* at 386-88. *See also* W. PROSSER, THE LAW OF TORTS § 117, at 804 (4th ed. 1971). The four categories, each depending on a different rationale and each punishing different acts, are:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Prosser, *supra* note 1, at 389.

4. *Id.* at 410.
5. *See, e.g.*, Rosenbloom v. Metromedia, 403 U.S. 29 (1971); Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967); Time, Inc. v. Hill, 385 U.S. 374 (1967); New York Times Co. v. Sullivan, 376 U.S. 254 (1964). *See also* pp. 1463-65 *infra*.

protection of the First Amendment.[6] In all suits for public disclosure of private information, publishers may well enjoy a complete defense of privilege under the First Amendment. If this is true, then there can be no constitutionally acceptable remedy for the injury caused by publishing private, true facts, and the public disclosure tort is unconstitutional on its face—an inference some legal scholars have already drawn.[7]

However, the analytical premises of the Court do not lead necessarily to that conclusion. Using the same premises, a First Amendment interest can be shown in *preserving* the public disclosure tort remedy, based on a First Amendment interest in the particular form of privacy which the tort protects.

I

The starting point for constitutional arguments both for and against the public disclosure tort is a theory of the First Amendment which the Supreme Court has articulated over the last decade. Beginning with *New York Times Co. v. Sullivan*[8] in 1964, the Court in applying the free speech guarantee has stressed the integral role of free speech in a democratic political system, and has uncovered a First Amendment interest in protecting a "system of freedom of expression."[9] In deciding the constitutionality of an individual utterance, therefore, the Court has taken into account not only the merits of the specific utterance but also its place in a constitutional system of speech. The Court's theory rests on the premise that free speech provides citizens with that "access to social, political, esthetic, moral and other ideas and experiences"[10] which citizens require in order to perform "[s]elf-governance."[11]

6. *See* p. 1468 & notes 27-31 *infra*.

7. *See* Marc Franklin, *A Constitutional Problem in Privacy Protection: Legal Inhibitions on Reporting of Fact*, 16 STAN. L. REV. 107 (1964). Others who have recognized the potential unconstitutionality of a public disclosure tort include T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 517 (1970); Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326, 336 (1966). *See also* Kapellas v. Kofman, 1 Cal. 3d 20, 35, 459 P.2d 912, 922, 81 Cal. Rptr. 360, 370 (1969).

8. 376 U.S. 254 (1964).

9. The phrase is the title of Professor Thomas Emerson's study of the Supreme Court's treatment of the First Amendment, T. EMERSON, *supra* note 7. Emerson posits that "[t]he root purpose of the First Amendment is to assure an effective system of freedom of expression in a democratic society." *Id.* at 17.

The Court itself has said that "[a] broadly defined freedom of the press assures the maintenance of our political system and an open society," Time, Inc. v. Hill, 385 U.S. 374, 389 (1967), and it has observed "a profound national commitment to the principle that debate on public issues should be uninhibited . . . ." New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964). Justice Black has called First Amendment guarantees "the heart of the system on which our freedom depends." American Communications Ass'n v. Douds, 339 U.S. 382, 453 (1950) (dissenting opinion).

10. Red Lion Broadcasting Co. v. F.C.C., 395 U.S. 367, 390 (1969).

11. Rosenbloom v. Metromedia, 403 U.S. 29, 41 (1971).

37-583 O - 74 - pt. 2 - 4

As Mr. Justice Brennan has acknowledged, the Court has developed its self-governance rationale for protecting an integrated system of First Amendment freedoms in light of the work of the late Alexander Meiklejohn.[12] In Meiklejohn's classic formulation,

> The First Amendment does not protect a "freedom to speak." It protects the freedom of those activities of thought and communication by which we "govern." It is concerned, not with a private right, but with a public power, a governmental responsibility.[13]

In other words, free speech is protected not for some intrinsic value of speech but because it is a necessary condition for the making of informed decisions about matters of government, decisions which all citizens in a democracy are called on to make. Speech provides information, the raw material from which citizens can make self-governing choices.

Although the Court has never set out the elements of the free expression system, its operation would seem to require two separate stages. Transmission of information from speaker to listener is only the first; the second is the application of that information—in the mind of the person who receives it—to the individual decisions of self-governance.[14] Both stages of the process are needed to achieve what, in the Court's view, the Constitution envisions: free individual choice by each citizen.

Yet the Court, in applying its concept of a free expression system, has concerned itself almost solely with the first stage of that system—the process of communicating information from speaker to listener. In

12. Brennan, *The Supreme Court and the Meiklejohn Interpretation of the First Amendment*, 79 HARV. L. REV. 1 (1965). Justice Black cites Meiklejohn in his concurrence in New York Times Co. v. Sullivan, 376 U.S. 254, 297 n.6 (1964).

13. Meiklejohn, *The First Amendment Is An Absolute*, 1961 SUP. CT. REV. 245, 255. Professor Emerson believes that a free expression system also serves the goals of individual self-fulfillment and the discovery of truth, independent of their relationship to governing process. T. EMERSON, *supra* note 7, at 6-7.

14. Although the Court has not hitherto viewed its system as involving two operative stages, Justice Douglas appeared to recognize an analogous division of First Amendment operation in his dissent in United States v. Caldwell, one of the three cases consolidated in Branzburg v. Hayes, 408 U.S. 665 (1972). After quoting from Meiklejohn, he argued:

> Two principles which follow from this understanding of the First Amendment are at stake here. One is that the people, the ultimate governors, must have absolute freedom of, and therefore privacy of, their individual opinions and beliefs regardless of how suspect or strange they may appear to others. Ancillary to that principle is the conclusion that an individual must also have absolute privacy over whatever information he may generate in the course of testing his opinions and beliefs . . . . The second principle is that effective self-government cannot succeed unless the people are immersed in a steady, robust, unimpeded, and uncensored flow of opinion and reporting which are continuously subjected to critique, rebuttal, and reexamination.

Id. at 714-15. Douglas' first principle is analogous to the second stage proposed here, and his second principle is analogous to the first stage.

the context of that first stage, the Court has recognized that participation of individuals in a free expression system can be inhibited, or chilled, in a variety of ways and that the result is to diminish the self-governing rights of at least those individuals.[15] It has therefore acted in the name of the First Amendment to forestall those potential inhibitory effects. But at the same time the Court has taken for granted the freedom from potential inhibition of the second stage—the listener's decision-making in light of received information—which begins after the communication between speaker and listener is complete. The Court's assumption seems to be that speech need only reach the listener's ear for the free expression system of democracy to operate successfully.[16]

Lamont v. Postmaster General[17] illustrates the distinction between inhibitions of the first stage and inhibitions of the second, and the Court's unwillingness to perceive the latter. In *Lamont,* the Court struck down a Post Office requirement that addressees of "Communist propaganda" had to request the "propaganda" in writing before it would be delivered. The Court's opinion focused on the hindrance to free speech which the written request represented: the hindrance to the successful act of communication between the person who mailed the "propaganda" and the intended recipient.[18] No mention was made of the effect on the addressees of knowing that the Post Office had identified them as recipients of subversive mail.[19] Knowing that they had been so identified, they might be inhibited from making a later self-governing choice, such as the choice to vote for a Communist political candidate. Under the *Lamont* facts, that chilling effect (an inhibition of the free expression system's second stage) seems a more likely and more worrisome possibility than the possibility that a written request requirement might impede the flow of speech (a first-stage inhibition). Yet the decision turns on the first-stage inhibition alone.

15. *See, e.g.,* Lamont v. Postmaster General, 381 U.S. 301, 307 (1965). *See also* note 26 *infra.*

16. The Court has often used the phrase "the right to receive information and ideas," *see, e.g.,* Kleindienst v. Mandel, 408 U.S. 753, 762-64 (1972); Stanley v. Georgia, 394 U.S. 557, 563 (1969). But it has invoked the right only to protect the act of communication between speaker and listener; the phrase has never been used to indicate any hearer's right to First Amendment protection in his subsequent decision-making. The "right to receive" appears to apply only to the same circumstances as the right to speak; the Court seems to use it as a substitute for the "right to speak" in cases where its sympathies do not lie with the speaker. In *Mandel,* for example, the speaker was a Belgian Marxist applying for permission to enter the United States; in *Stanley* the speakers were makers of pornographic films.

17. 381 U.S. 301 (1965).

18. *Id.* at 307.

19. At one point, the Post Office was keeping a central list of these recipients, although it claimed to have discontinued the practice before trial. 381 U.S. at 303.

A possible reason for the Court's disregard of the free expression system's second stage is that the threat of inhibition to the second stage is much harder to imagine than the threat of inhibition to the first. If inhibition stems from public disapproval of unpopular beliefs, the speaker in the first stage is obviously vulnerable. Many people know what he believes, because he tells them. He invites antipathy, and perhaps suppression. The second stage of the system, on the other hand, takes place entirely within the mind of the individual, and in performing it the individual attracts no attention; he is insulated from public knowledge and potential disapproval. Perhaps a hostile public might not like the decisions he was reaching and might want to inhibit him from reaching such decisions, if it could know; but how would it find out? The insulation of the individual against the chilling of his self-governing decisions is thus his ability to prevent public knowledge about himself.

Privacy is the name which the public disclosure tort cases give to the individual's ability to control information about himself.[20] And with those cases, this concept of the nature of privacy is introduced into the law. Privacy understood in this special sense—as control of information about oneself—is prerequisite to the operation of the free expression system's second stage, at least if that second stage is to operate with the freedom from inhibition which has been firmly guaranteed to the first stage.

One simple recognition of privacy's importance to self-governance is the curtain on the voting booth. But the shelter of privacy is needed for more than the casting of the formal vote, both because there are other ways of registering self-governing choices and because the process of reaching a decision does not take place only at the moment of formal choice-registering; it is a continuous process which extends from the receipt of each item of information from a speaker to each choice, formal or informal, which the citizen registers.[21] He who performs his listening and deciding functions in a glass house is coerced by public opinion, whether anyone is actually looking in or not. If every magazine

20. *See, e.g.*, Banks v. King Features Syndicate, 30 F. Supp. 352, 353-54 (1939) (x-rays of plaintiff's pelvis); Mau v. Rio Grande Oil, Inc., 28 F. Supp. 845, 846 (1939) (plaintiff's experience as holdup victim); Cohen v. Marx, 94 Cal. App. 2d 704, 705, 211 P.2d 320, 321 (1949) (prizefighter's losing record); Melvin v. Reid, 112 Cal. App. 285, 289-90, 297 P. 91, 92-93 (1931) (plaintiff's former career as prostitute); Cason v. Baskin, 155 Fla. 198, 207-11, 20 So. 2d 243, 247-48 (1945) (biographical sketch of plaintiff); Trammel v. Citizen News Co., 285 Ky. 529, 531, 148 S.W.2d 708, 709 (1941) (plaintiff's debt to grocer). *See also* Prosser, *supra* note 1, at 392-98. For criticism of the public disclosure tort, see Kalven, *supra* note 7, at 333-39.

21. *Cf.* Meiklejohn, *supra* note 13, at 255-57.

he reads, every rally he attends, every person he speaks to might somehow become a matter of public knowledge, he would feel inhibiting pressure.[22] The pressure is the same as that felt by a member of the NAACP in Alabama when he fears that the fact of his membership will be publicized.[23] The Court itself, in discussing the threat to First Amendment freedoms which might result from the House Un-American Activities Committee forcing one admitted Communist sympathizer to identify others, has noted:

> [T]hose who are identified by witnesses and thereby placed in the same glare of publicity are equally subject to public stigma, scorn and obloquy. *Beyond that, there is the more subtle and immeasurable effect upon those who tend to adhere to the most orthodox and uncontroversial views and associations in order to avoid a similar fate . . . .*[24]

The effect described is the response of a citizen uncertain of his privacy as he goes about making self-governing decisions within the system of freedom of expression. A more highly developed form of the same coercion can be found in a citizenry watched over by a thought police, where the threat—that the manifestations of an individual's thinking will be collected and examined—is made overt.[25] No curtailment of the first stage of that system is necessary to erode it; inhibiting the second stage is just as effective. And since the participants in the latter stage are more numerous and more timid than speakers in the former, effective methods of control can be less direct and less conspicuous than those which successfully inhibit the first stage of the system's operation. Not only the privacy of the decision-making process but also confidence in that privacy is at stake; pulling back the curtain on one voter

22. The most eloquent statement of the point occurs in Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964) [hereinafter cited as Bloustein, *An Answer to Dean Prosser*]. The mere collection of such data may constitute an infringement of privacy even apart from the threat of inhibition. *See* Nader v. General Motors Corp., 25 N.Y.2d 560, 573, 255 N.E.2d 765, 773, 307 N.Y.S.2d 647, 658 (1970) (Breitel, J., concurring). *But see* T. EMERSON, *supra* note 7, at 556.

23. *See* N.A.A.C.P. v. Alabama, 357 U.S. 449 (1958). In that case the Supreme Court said that

> compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] . . . effective . . . restraint on freedom of association . . . . This Court has recognized the vital relationship between freedom to associate and privacy in one's association . . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.

Id. at 562. *See also* Louisiana v. N.A.A.C.P., 366 U.S. 293 (1961).

24. Watkins v. United States, 354 U.S. 178, 197-98 (1957) (emphasis added).

25. For the effect on privacy of totalitarian government, *see, e.g.*, A. WESTIN, PRIVACY AND FREEDOM 23 (1967); Kalven, *supra* note 7, at 326.

threatens others.[26] Thus, if a free expression system is to be maintained, the First Amendment has an interest in protecting the privacy of the individual.

Assuming that privacy consists only in the individual's control of information about himself—his keeping it from the knowledge of others—then the First Amendment interest in that privacy will extend only to certain types of information: that information which, if released, would inhibit the individual's freedom to reach decisions of self-government. Perhaps this category is only a narrow one. But in free speech cases involving libel suits, the Supreme Court has discovered self-governing relevance in many kinds of information, not merely the small category of information which has obvious "political" relevance.[27] It has held that the First Amendment has an interest in protecting published information whether it be opinion or fact,[28] whether the fact be true or false,[29] whether the subject of the information be public official or private citizen,[30] and whether the subject be well-known or obscure.[31] If the inquiry is reversed and instead becomes the First Amendment (*i.e.*, self-governing) relevance of information *to the person whom it involves,* it is hard to see how the Court could take a narrower view. In both cases the question is what kinds of information—what content—might have an effect on the self-governing decisions of citizens, and the answer in both cases should be the same.

In *Time, Inc. v. Hill*,[32] for example, the Court held that publication of James Hill's name in connection with the play based on his experiences was privileged because, in effect, knowledge of that information might be useful to the members of the public in arriving at decisions of self-government.[33] But, James Hill should be able to claim, the *privacy* of that information is also important to *his* decision-making; when the information is exposed, he is inhibited. He might have planned to accept public office as a special prosecutor of organized

26. The threat that many citizens will be inhibited through the direct inhibition of only one is a well-established piece of First Amendment doctrine. *See, e.g.*, Baird v. State Bar, 401 U.S. 1, 6 (1971); Keyishian v. Bd. of Regents, 385 U.S. 589, 603-04 (1967); Lamont v. Postmaster General, 381 U.S. 301, 307 (1965). *But see* Laird v. Tatum, 408 U.S. 1, 10-11 (1972).

27. *See* note 15 *supra*. *See also* T. EMERSON, *supra* note 7, at 540-41. *But see* Bork, *Neutral Principles and Some First Amendment Problems*, 47 INDIANA L.J. 1, 27 (1971).

28. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 271-73 (1964).

29. *Id.* at 271-72.

30. Rosenbloom v. Metromedia, 403 U.S. 29, 31-32 (1971); Curtis Publishing Co. v. Butts, 388 U.S. 130, 155, 163-64 (1967).

31. Rosenbloom v. Metromedia, 403 U.S. 29, 31-32 (1971).

32. 385 U.S. 374 (1967).

33. "We have no doubt that the subject of the Life article, the opening of a new play linked to an actual incident, is a matter of public interest." *Id.* at 388.

crime; now, the public's knowledge that his family has been held hostage once before makes him fear that a mobster might think to try it again. He might have been about to petition his elected representatives for lighter kidnapping penalties; now he would be ridiculed. He intended to see the play himself; now he would be the center of unwanted attention. Most important, his confidence in the privacy of his life in general is shaken; if the fact that he was held hostage can be told, what about his atheism, or his check to the Black Panthers?[34] The point is not that any item of news which is publishable is also necessarily a valuable part of someone's privacy; it is that any *type* of information has the potential to be either. The First Amendment has an interest in protecting a broad range of speech; it has also a parallel interest in protecting a broad range of privacy.

Both First Amendment interests are present in the paradigm public disclosure tort situation,[35] where a plaintiff's privacy claim will always face the claim of the defendant publisher that the information published is in the public interest and therefore is privileged.[36] Hence, such cases would seem to pose a rare constitutional dilemma: the need to choose between two opposing claims, both of which arise from the same constitutional provision. Each party can demonstrate an injury to the free expression system of self-government if the other is allowed his way, and apparently one claim can be upheld only at the expense of the other. The Court has not yet acknowledged this conflict; instead it has automatically upheld the claim of the publisher when that claim has substance.[37]

34. None of these inhibitions by itself is overwhelming, and it might be argued that they ought not to be taken into account at all in determining First Amendment freedoms. Mr. Justice Black appears to take this view in Time, Inc. v. Hill, 385 U.S. at 399-400 (concurring opinion). One can also deny that such inhibitions are possible, if one believes that "Freedom to think is absolute of its own nature; the most tyrannical government is powerless to control the inward workings of the mind." Jones v. Opelika, 316 U.S. 584, 618 (1942) (Murphy, J., dissenting), *adopted as the opinion of the Court in* Jones v. Opelika, 319 U.S. 103 (1943).

This Note does not argue that the inhibitions suggested should outweigh substantial free speech interests of the publishers, but only that consideration should be given to the inhibitory effect of allowing publication as well as to the inhibitory effect of punishing it. In cases where the free speech interest to the public is small, the privacy interest to the individual might be relatively large. *See* pp. 1471-72 *infra*.

35. *See* p. 1462 *supra*.

36. The discussion is hypothetical because in no public disclosure case to date has the constitutional defense been raised. The closest example is Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940), in which a newsworthiness privilege was successfully asserted; but because of the peculiarities of the New York "privacy" statute, that state cannot be said to have a proper public disclosure tort action. *See* note 83 *infra*. The most important defect of the New York law, from the standpoint of a public disclosure tort action, is that truth is a defense. The same confusion arose in Time, Inc. v. Hill and was discussed by Justice Fortas. His dissenting opinion stressed that the First Amendment should not preclude the protection of a right of privacy. 385 U.S. at 412. *See also* the concurring and dissenting opinion of Justice Harlan, *id.* at 404.

37. *See, e.g.*, Rosenbloom v. Metromedia, 403 U.S. 29, 48 (1971).

One possible accommodation of the conflicting First Amendment claims in the public disclosure case might be made by focusing on the issue of names and separating them from the news items in which they appear. The crux of an individual's privacy is not the disclosure of private information by itself, but the linking of that information to the individual in question, by name or otherwise. If it is possible that a piece of information is relevant to the self-governing choices of the public, but that the identity of the subject of that information is not, then at least in such cases both claims can be satisfied.

For example, publishing the fact that a young woman in Kansas City suffers from a disease of compulsive overeating does not infringe the privacy of the woman; publishing her name and a photograph showing her face certainly does.[38] On the other hand, the value of that news item to the self-governing public lies primarily in the fact of the disease and little if at all in the identification of the sufferer. The woman's condition is medically interesting and the fact of its existence might be relevant in reaching such decisions as whether to approve a hospital bond issue. But at the same time, the fact that the woman is Mrs. Dorothy Barber might not have any relevance to the self-governing decisions of the same public. Or, if it is somehow relevant, the relevance is of a much lower order of magnitude.

Of course, there are cases in which the identity of a person involved in a news event is itself relevant to the purposes of self-government, as when the person holds public office or a place in the public eye.[39] But in many cases, the identification of the subject of a published news item is not of significant value; it is unlikely to have any effect on the political choices which the reader will make. Most suits for injury caused by public disclosure of private facts have focused on the single issue of identification, conceding the public news value of a prostitute's life,[40] a genius' decline,[41] or schoolchildren's disruptive behavior,[42] but claiming that the privilege to publish does not extent to the name of the individuals involved when they are not themselves currently public figures.

In public disclosure cases in which the plaintiff is not well-known,

38. *See* Barber v. Time, Inc., 348 Mo. 1199, 159 S.W.2d 291 (1942). For a general discussion, see Briscoe v. Readers' Digest Ass'n, 4 Cal. 3d 529, 537, 483 P.2d 34, 40, 93 Cal. Rptr. 866, 872 (1971).

39. *See* Kapellas v. Kofman, 1 Cal. 3d 20, 36, 459 P.2d 912, 922, 81 Cal. Rptr. 360, 370 (1969). *See also* Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967); New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

40. Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931).

41. Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940).

42. Doe v. McMillan, 41 U.S.L.W. 4752 (U.S. May 29, 1973).

the First Amendment interest of the public, operating through the publisher, is satisfied by the publication of the fact or event; the First Amendment interest of the subject is satisfied if the publisher refrains from identifying him. Hence there is no constitutional objection to preserving a tort remedy for the plaintiff if the publisher does identify him and thereby injures his privacy. But this result can only be reached if the constitutional privilege to tell the public a piece of news is judged separately from the constitutional privilege to tell the public who was involved.[43]

Edward Bloustein has already suggested a similar method of accommodating the First Amendment and the public disclosure tort. He conceives of the relevance issue as a limit on the First Amendment, thus providing room beyond the boundaries of free speech for the operation of privacy tort law.[44] Privacy, in his view, takes up where the free expression system leaves off.[45] But in the context developed above, Bloustein's formulation is incomplete. It is not enough to say that protection will be allowed only in cases too trivial to enter the First Amendment arena. The difficult and important cases are those in which the First Amendment interests in privacy and speech compete. A court cannot dispose of the First Amendment issue by deciding merely that the name of an individual is "of legitimate public interest"; if it so decides, it must then balance the resulting First Amendment interest in publication of the name with the First Amendment interest in protecting the privacy of the individual.[46] In doing so, it should consider the net effect of allowing publication (or protecting privacy) on the free expression system at large. The Court has said in other contexts that the constitutional interest in unrestricted speech can be outweighed;[47] in some

43. To reach such decisions, of course, courts must overcome the misleading slogan that "names are news," which many have taken as a normative prescription. *See* Comment, *The Right of Privacy: Normative-Descriptive Confusion in the Defense of Newsworthiness*, 30 U. Chi. L. Rev. 722 (1963). That "names are news" is apt commercial description has been endlessly demonstrated, but commercial fact should be irrelevant to the constitutional decision at stake: Does the name of a given person, linked to some information, have value to those who hear or read the resulting news item, in that they will find it useful in arriving at the decisions of self-government?

44. Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well?*, 46 Texas L. Rev. 611, 626 (1968).

45. Though he deals with a privacy of broader definition, Emerson also suggests that First Amendment rights and privacy rights should apply in mutually exclusive areas. T. Emerson, *supra* note 7, at 548. For him as for Bloustein, the problem then becomes one of drawing the boundary line.

46. Of course, if the court decides that the name is not "of legitimate public interest," the publisher has no defense of privilege and the plaintiff's cause of action in tort is good. *See, e.g.*, Briscoe v. Readers' Digest Ass'n, 4 Cal. 3d 529, 483 P.2d 34, 93 Cal. Rptr. 866 (1971).

47. *See, e.g.*, Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942). *Cf.* Wright, *Defamation, Privacy, and the Public's Right to Know*, 46 Texas L. Rev. 630, 634 (1968).

cases it might well be outweighed by the First Amendment interest in privacy.

Evaluating the constitutionality of a given public disclosure suit should involve a calculation as to which result will best serve *the system* of which both claimants are a part and to which both appeal. The calculation may well come out in favor of publication, but it should be a calculation and not a blanket assertion that the First Amendment is always best served by the privileged publication of newsworthy items of information. At least in the area of identification, as suggested above, the calculation of effect on a free expression system might well produce an opposite result. If so, a public disclosure tort action addressed to the unauthorized use of names cannot be automatically invalidated under the First Amendment.[48]

II

The constitutional argument for the public disclosure tort suggests solutions to two major problems in current privacy law. First, the argument provides a conceptual definition of the privacy interest at stake; and second, it provides a doctrinal justification for protecting that interest in law. Common law privacy doctrine has failed to supply either of these. Prosser's definitive article on the common law of privacy established public disclosure as one of the four recognized categories of tort actions addressed to the protection of privacy.[49] But Prosser's classification, based on differences in the kind of injury involved, was only descriptive; it offered no justification for the different types of recovery. And though his categories have been widely influential, critics have complained that his most original category—the public disclosure action —lacks a conceptual foundation.[50]

Of Prosser's four categories of privacy actions, three rest on venerable tort doctrine. False light is a homologue of libel; appropriation uses the reasoning and damage measure of personal property law; and intrusion expands on the law of trespass *quare clausum fregit*.[51] In each cate-

48. The tort might well be held unconstitutional as applied in a specific case. In New York Times Co. v. Sullivan, for example, the Alabama libel tort was so held. But the tort was not and could not have been held unconstitutional on its face, and the same would apply to the public disclosure tort in a constitutional challenge.

49. Prosser, *supra* note 1.

50. *See, e.g.*, Kalven, *supra* note 7, at 331-32.

51. For the relationship of false light and libel, see Wade, *Defamation and the Right of Privacy*, 15 VAND. L. REV. 1093 (1962). *See also* Kalven, *supra* note 7, at 332, 339-41. For the use of property concepts in appropriation cases, compare the majority with the dissenting opinion in Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902). *See also* O'Brien v. Pabst Sales Co., 124 F.2d 167, 170 (5th Cir. 1941) (dissenting opinion). *See generally* Prosser, *supra* note 1; Bloustein, *An Answer to Dean Prosser*, *supra* note 22.

gory the central injury has long been recognized in law, and calling it an injury to "privacy" is a semantic, not a legal, innovation. The public disclosure tort, on the other hand, presents a true conceptual novelty: the idea that mere publication of accurate data about a person might cause him legal injury.[52]

The false light action protects against injuries to reputation only; and, as with libel, truth is a defense. It therefore gives the individual no right to control accurate information about himself. Any relationship of the tort action to a concept of privacy is tenuous.

The action for appropriation of name or likeness protects against the publication of true information about the individual, but it concerns only that information on which the individual might have capitalized himself. The injury is a commercial one; the action protects less a right to privacy than a right to publicity.[53] Since recovery under the appropriation tort depends on the economic injury suffered,[54] those who suffer the largest loss of privacy through publication of their names and faces—those who have been utterly unknown before the publication—stand to recover least.[55]

The intrusion tort comes closer than false light or appropriation to offering a satisfactory definition of privacy. It protects the individual's right to control access to his immediate surroundings, and thus defines

52. Before the famous article by Warren and Brandeis appeared in 1890, this was a suggestion virtually unheard in the law. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Seventy-five years later, the law still often fails to recognize injury to privacy in the absence of trespass, bodily injury, theft, or money damages. *See* Ruebhausen & Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1185 (1965). *See generally* 1 F. HARPER & F. JAMES, THE LAW OF TORTS § 9.5, at 678-79 (1956).

53. Prosser, *supra* note 1, at 406-07. *See also* Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROB. 203 (1954); Note, *The Right of Publicity: A Doctrinal Innovation*, 62 YALE L.J. 1123 (1953).

54. There can be no economic measure of a genuine injury to privacy; the worth of a man's privacy cannot vary with the commercial value of his name or face in the marketplace. Yet just this distortion has crept into nearly all privacy tort recoveries because elements of appropriation actions have not been kept separate from those of other suits classed under the privacy heading. *See* Bloustein, *An Answer to Dean Prosser*, *supra* note 22, at 977-91.

Damage measure is a long-standing problem in privacy tort law which this Note does not purport to solve. Justices Harlan and Fortas have suggested an actual or compensatory damage measure. Rosenbloom v. Metromedia, 403 U.S. 29, 66 (1971) (Harlan, J., dissenting); Time, Inc. v. Hill, 385 U.S. 374, 420 (1967) (Fortas, J., dissenting). But for a discussion of the difficulty of measuring the extent of an injury to personality caused by publication, see Shapo, *Media Injuries to Personality; An Essay on Legal Regulation of Public Communications*, 46 TEXAS L. REV. 650, 658-67 (1968). For criticism of privacy damages as conjectural, see Kalven, *supra* note 7, at 334. For the observation that the injury for which privacy damages are supposed to compensate is irreparable, see Bloustein, *An Answer to Dean Prosser*, *supra* note 22, at 1002-03. *See generally* W. PROSSER, THE LAW OF TORTS § 117, at 815 (4th ed. 1971).

55. Perhaps in recognition of this problem, California has recently imposed a minimum liability of $300 for commercial use of a person's name, photograph, or likeness. CALIF. CIVIL CODE § 3344(a) (West Supp. 1972). The appropriation tort is the only one of the four privacy torts to be codified in state statutes. *See* W. PROSSER, *supra* note 54, § 117, at 805.

privacy as control of physical space. Physical space is an important and well-recognized element of privacy, and spatial metaphor dominates legal thinking about the subject; for example, we most commonly refer to any infringement of privacy as an "invasion." Yet on the basis of its definition of privacy, the intrusion tort draws distinctions which seem to have nothing to do with privateness. In *Nader v. General Motors Corp.*,[56] for example, "mere gathering" of private information was held not punishable unless the gatherer was "unreasonably intrusive." Though Nader claimed that he was shadowed by detectives, that a dossier on his private life was compiled through observation and interviews with acquaintances, and that his bank accounts and tax returns were pried into, only wiretapping and eavesdropping were held to give rise to a cause of action for intrusion.[57]

The public disclosure tort, by finding legal injury in the mere act of publishing accurate data about a person, protects something which is farther from traditional tort theory, and perhaps closer to a satisfactory concept of privacy. The actual content of a person's privacy is a subjective matter over which people inevitably disagree, but even as they disagree they can share a common concept of how privacy works and what purpose it serves. Scholars who have sought a conceptual definition of privacy have not been unanimous, but a common theme appears in many of their efforts: that privacy reflects a psychological need of the individual to keep some core of personality to himself, outside the notice of society.[58] The ultimate value at stake has been variously described—human dignity, individuality, and autonomy have been suggested—but in each description the point is that it is kept from the awareness of others at the will of the individual.[59] Nor is privacy simply rigid secrecy; it is essential that the individual be free to reveal parts of his selfhood to chosen others.[60] Charles Fried considers this gift of selfhood to be the essence of relationships of love, friendship, trust, and respect, and argues that these intimate relationships cannot exist without the confidence of the individual that only his chosen intimates will possess intimate knowledge of him; in other words, intimacy depends on the inaccessibility of one's private self to society at large.[61]

56. 25 N.Y.2d 560, 255 N.E.2d 765, 307 N.Y.S.2d 647 (1970).
57. 25 N.Y.2d 560, 564-71, 255 N.E.2d 765, 767-71, 307 N.Y.S.2d 647, 650-56 (1970).
58. H. Arendt, The Human Condition 22-78 (1958); E. Goffman, The Presentation of Self in Everyday Life (1959); A. Westin, *supra* note 25, at 8-63; Bloustein, *An Answer to Dean Prosser*, *supra* note 22, at 1002-03; Arnold Simmel, *Privacy is Not an Isolated Freedom*, 13 NOMOS 71, 72-74 (1971); Warren & Brandeis, *supra* note 52, at 205. *See also* Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) (Stewart, J., concurring).
59. *See* note 58 *supra*.
60. Shils, *Privacy: Its Constitution and Vicissitudes*, 31 Law & Contemp. Prob. 281, 281-83 (1966).
61. Fried, *Privacy*, 77 Yale L.J. 475 (1968).

Control of information about oneself is thus the essence of privacy: "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[62] The public disclosure tort action—which punishes the unjustified exposure through mass publication of the data of an individual's life—contains the only direct recognition which the law has given to that non-libel, non-territorial, non-commercial claim.[63]

III

Constitutional law shares the conceptual weakness of common law in the privacy area. The Supreme Court has declared that the Constitution protects a right to privacy, but the supporting analysis offers no hint as to how that protected privacy might be defined. Other constitutional grounds which have been set forth present better possibilities of definition, but the rights so defined are far too narrow and qualified to serve as a satisfactory "right to privacy."

As the opinions in the recent abortion cases[64] confirm, the Court's primary analytical model of privacy is that which appears in the plurality opinion of Mr. Justice Douglas in *Griswold v. Connecticut*.[65] In *Griswold*, Justice Douglas collected the various existing constitutional doctrines which might be considered to protect some specific interest in privacy—including the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments—and, rather than relying on any one of them, declared that their sum resulted in a constitutional interest in privacy in general.[66] Justice Douglas' argument, though in form an argument by analogy to existing constitutional rights,[67] in effect contended for the establishment of a new and independent constitutional right. The protection of privacy is incident to several constitutional goals; therefore it should be a goal itself. The formula reflects the belief of Pro-

62. A. Westin, *supra* note 25, at 7. Similar definitions are offered in Ruebhausen & Brim, *supra* note 52, at 1189-90, and Shils, *supra* note 60, at 282.

63. If courts come to accept the separate doctrinal underpinning of the public disclosure tort, they can begin to untangle some of the confusions of privacy law in general, an area whose state of organization one judge has likened to "a haystack in a hurricane." Ettore v. Philco Television Broadcasting Co., 229 F.2d 481, 485 (3d Cir. 1956) (Biggs, C.J.). Plaintiffs would be able to seek relief directly for injuries to their privacy without having to claim injury to reputation or pocketbook as they often must at present. *See* note 52 *supra*. Hybrid privacy actions would cease to distort libel law. *Cf.* Wade, *supra* note 51. *See also* Kalven, *supra* note 7, at 335. Finally, courts would be able consistently to separate economic injury from injury to privacy and relegate them to separate causes of action. *Cf.* note 54 *supra*.

64. Roe v. Wade, 93 S. Ct. 705 (1973); Doe v. Bolton, 93 S. Ct. 739 (1973).

65. 381 U.S. 479 (1965).

66. Griswold, 381 U.S. at 480-86.

67. *See* Mitchell Franklin, *The Ninth Amendment As Civil Law Method and its Implication for Republican Form of Government:* Griswold v. Connecticut; South Carolina v. Katzenbach, 40 Tulane L. Rev. 487, 490-91 (1966).

fessor Emerson, who argued the case for the *Griswold* plaintiffs before the Supreme Court, that only a newly declared constitutional right which "cuts across" other constitutional rights can adequately protect individual privacy.[68]

The First, Fourth, Fifth, Ninth and Fourteenth Amendment argument of *Griswold*—perhaps streamlined in *Roe v. Wade* to a Fourteenth Amendment argument alone[69]—presents the advantage of breadth. However, the definitions of privacy which the *Griswold* approach offers are at best descriptions of a widely shared emotional attitude.[70] Analytically, the reasoning of *Griswold* and *Wade* offers no guidance for separating what privacy is from what it is not; it offers no generalizable definition of the right it is used to protect. Indeed, the extreme breadth of the *Griswold* analysis has produced utmost caution in courts called on to apply it,[71] and even *Wade* extends the resulting right only within the area of intimate bodily conduct. Confining the right to privacy inside that area is sanctioned by custom, but not by anything in the reasoning of the decisions.

An alternative to the form of argument which identifies privacy as a wholly new constitutional right is one which discovers that privacy is incident to a constitutional right already well established. If that established right is to be fully realized, the argument runs, privacy in some form must be protected. Each of the doctrines which Douglas col-

68. T. EMERSON, *supra* note 7, at 556. Professor Emerson's brief in *Griswold* invoked the First Amendment in support of a constitutional right to privacy, but it did so only in a limited context. Brief for Appellants at 79-80, Griswold v. Connecticut, 381 U.S. 479 (1965). There is no suggestion that a constitutional right to privacy might rest on the First Amendment or its system of freedom of expression; indeed, the First Amendment was not included in the summary list of constitutional provisions from which a right to privacy was said to emanate. *Id.* at 12.

69. Roe v. Wade, 93 S. Ct. 705, 727, 733-36 (1973) (Stewart, J., concurring); *id.* at 755 (Burger, C.J., concurring). *But cf. id.* at 737-39 (Rehnquist, J., dissenting). Two of the *Griswold* opinions also located the right to privacy under the Due Process Clause of the Fourteenth Amendment. 381 U.S. at 499-500 (Harlan, J., concurring); *id.* at 502-03 (White, J., concurring).

70. The most familiar such definition of privacy is "the right to be let alone." *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 494 (Goldberg, J., concurring), *quoting* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Justice Goldberg offers another in *Griswold:* "the integrity of [family] life." 381 U.S. at 495. *Cf.* Justice Black's attack in *Griswold* on the dangers of defining privacy too narrowly, 381 U.S. at 509 (dissenting opinion).

More usually, the Court's attempted definitions of privacy reflect only the Court's own sense that the subject is important. Examples of these include "the right most valued by civilized men," *Griswold*, 381 U.S. at 494 (Goldberg, J., concurring), *quoting Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting); "a right . . . older than the Bill of Rights," *Griswold*, 381 U.S. at 486; and "personal rights 'implicit in the concept of ordered liberty,'" Roe v. Wade, 93 S. Ct. at 726, *quoting* Palko v. Connecticut, 302 U.S. 319, 325 (1937).

71. *See* T. EMERSON, *supra* note 7, at 557. *Cf.* Hufstedler, *The Directions and Misdirections of a Constitutional Right of Privacy*, 26 RECORD OF N.Y.C.B.A. 546, 559 n.59 (1971).

lected in *Griswold* offers such an analysis.[72] And though *Griswold* may stand for the proposition that no one of them alone is adequate to support a right to privacy,[73] one in particular has seemed promising.

In her 1971 Cardozo Lecture, Judge Shirley Hufstedler set out an argument for deriving a broad constitutional protection of privacy from the Fourth Amendment prohibition of unreasonable searches and seizures.[74] Judge Hufstedler argued that the Fourth Amendment (and to a lesser extent the Fifth as well) was drafted to prevent penetrations of individual privacy, and that to realize that goal a broad interpretation should be given to the words "searches and seizures."

> Were that course taken, any governmental probe, corporeal or incorporeal, designed to uncover or to disclose information about a person would be a "search." The question whether the search was permissible would turn on its reasonableness.[75]

In effect, Judge Hufstedler proposed a constitutional analogue to the torts of intrusion and appropriation.

A Fourth Amendment "right to privacy,"[76] however, does not protect the substance of one's privacy; it merely prevents certain methods of obtaining that substance.[77] A reasonable search or seizure would presumably be constitutional no matter what the content of the private information revealed, nor would the content of that information necessarily affect the judgment of what is reasonable. In other words, the Fourth Amendment offers no definition of the content of its right to privacy, other than a reflexive one: it is that which is violated by an unreasonable search or seizure. Although the Supreme Court has repeatedly denied that the Fourth Amendment protects the privacy of places rather than people, it has yet to produce a Fourth Amendment holding which does not depend on the nature of the place where the unreasonable search or seizure took place. To the extent that privacy

72. These include the types of privacy protected by the First, Third, Fourth and Fifth Amendments, 381 U.S. at 484. Douglas seems to gloss over the Due Process Clause of the Fourteenth Amendment. *Id.* at 482. He does not do more with the Ninth Amendment than to quote it. *Id.* at 484.

73. The First Amendment rights which Douglas recounts—freedom of schooling and freedom of association—are subordinate to the express free speech guarantee, and they act to secure it. The Third Amendment protects the privacy of the home, if at all, only against the specific threat of being forced to quarter soldiers in peacetime. The Fourth Amendment protects privacy only as an incident to the prohibition against unreasonable searches and seizures. The Fifth Amendment's "zone of privacy" is subordinate to the operation of the Self-Incrimination Clause.

74. Hufstedler, *supra* note 71.

75. *Id.* at 561-62.

76. *See, e.g.*, United States v. White, 401 U.S. 745, 751, 752 (1971).

77. *See* Katz v. United States, 389 U.S. 347, 350 (1967).

means something other than that which happens in private places, a Fourth Amendment rationale is inadequate to protect it.[78]

Both the *Griswold* doctrine and the narrower doctrines which go to make it up reflect the Supreme Court's concern with the protection of individual privacy, and all of them help to protect privacy to some extent. But each fails to provide an adequate concept of the nature of privacy: how it arises, and what its characteristics are. Until the Court can say what privacy is, at least in conceptual terms, constitutional protection of privacy will be haphazard.

IV

Although the First Amendment analysis of the public disclosure tort generates a conception of privacy which comes closer than the conceptions of current tort and constitutional law to describing what privacy is and to making it susceptible to the application of legal doctrine, the claim which results is limited. The analysis discovers only a constitutional *interest* in privacy, not a constitutional *right* to have it protected in all cases. It does not yield a "First Amendment right to privacy" which can be placed next to the constitutional privacy rights which already exist.[79]

The first drawback to asserting the interest as a "right" is the narrow boundary within which it can be applied. It arises only within the constitutional structure of a free expression system. And in every case of public disclosure, the publisher has access to free expression claims which also serve the system. Since the individual's privacy is secured only at the expense of the free speech right of the publisher, it cannot grow too large. The First Amendment privacy interest is only in preventing the identification of an individual with information published,

78. This proposition might appear to be contradicted by Katz v. United States, which extended protection to a public telephone booth. But the Court held that Katz was protected against being overheard in a public telephone booth because he "justifiably relied" on the booth to protect his privacy; in other words, he temporarily constituted a private space from an apparently public one. *Id.* at 352-53. The distinction is made clearer in United States v. White, 401 U.S. 745 (1971), in which the Court held that *Katz* did not apply to an informer who takes a concealed transmitter into a suspect's home. Though the suspect obviously relied on the privacy of his home in talking to the informer, the Court found his reliance unreasonable. *Id.* at 753. Under the Fourth Amendment, privacy seems to depend on what one ought to expect about the characteristics of one's surroundings. If, on the other hand, the Court in *White* was considering privacy to be the control of information about oneself, its holding means that limited dissemination of information about oneself is unprotected; if you tell one person, everyone has a right to know. But recall Fried's discussion of the value of being able to limit the sharing of private information, note 61 *supra*.

79. For a summary of the Court's many constitutional privacy rights, see Roe v. Wade, 93 S. Ct. 705, 726-27 (1973).

and even then only after weighing the net effect on the free expression system.[80]

The second drawback is a state action problem. Since it is a private publisher who most often threatens to infringe individual privacy through a publication, the individual probably cannot assert his constitutional claim against that publisher directly;[81] he must rely on the indirect protection of a common law tort suit,[82] after the offending publication.[83] Moreover, not all states recognize a public disclosure tort in their common law;[84] in those which do not, the individual would have no mechanism at all through which to assert his claim for protection. A "First Amendment right to privacy" would thus depend for its existence on state courts or legislatures, a situation which the Court—if it were to recognize the "right" at all—would be unlikely to find satisfactory.[85]

Though a First Amendment analysis does not by itself justify the enforcement of a constitutional right to privacy, it nevertheless underscores the weaknesses of existing constitutional privacy doctrine. The analysis directs attention to the one form of privacy which the law, both common and constitutional, has so far been unable to protect successfully: the non-corporeal, non-quantifiable right to control of information about oneself, based on the content of the information rather

80. *See* pp. 1470-72 *supra*.

81. If a state agency is the publisher, presumably the publication is state action. *See, e.g.*, Burton v. Wilmington Parking Authority, 365 U.S. 715, 721-26 (1961). In that event, the individual could assert his First Amendment rights against the state directly, claiming state inhibition of his freedom of decision-making.

82. If the public disclosure tort were codified in state statute, it might be argued that a refusal by state courts to enforce the resulting state right of privacy might itself be sufficient state action to create federal jurisdiction. At present, however, the public disclosure tort exists only at common law. *See generally* W. Prosser, The Law of Torts § 117, at 809-12 (4th ed. 1971).

83. Nothing in this discussion is intended to suggest the propriety of a prior restraint of the publisher. *Cf.* Organization for a Better Austin v. Keefe, 402 U.S. 415 (1971); Near v. Minnesota, 283 U.S. 697 (1931). *See also* New York Times Co. v. United States, 403 U.S. 713 (1971).

The individual's dependence on state laws to protect his federal constitutional rights is less startling than it seems; even the right to free speech depends to an extent on state laws prohibiting, for example, assault and battery. If a speaker were not protected by state law against being pummeled every time he opened his mouth, or if a newspaper or radio station could not use state law to prevent its equipment from being destroyed by a displeased audience, freedom of speech and of the press would be effectively curtailed.

84. The number of states which recognize something like a public disclosure tort is uncertain. *See* note 3 *supra*. Some states, however, explicitly refuse to do so. New York, for example, has consistently refused to recognize such a right since the decision of Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902); instead the state legislature passed a statute, N.Y. Civ. Rights Law §§ 50, 51 (McKinney 1948), which more nearly fits the pattern of an appropriation tort. *See* Prosser, *supra* note 1, at 401. *Cf.* Time, Inc. v. Hill, 385 U.S. 374, 411-20 (1967) (Fortas, J., dissenting).

85. *Cf.* Rosenblatt v. Baer, 383 U.S. 75, 84 (1965), *citing* Pennekamp v. Florida, 328 U.S. 331, 335 (1946).

37-583 O - 74 - pt. 2 - 5

The Yale Law Journal Vol. 82: 1462, 1973

than the circumstances of its escape from one's control. Furthermore, the analysis suggests how privacy in that form might be integrated into a system of constitutional rights. The focus on the importance for privacy of information *qua* information, without regard to whether its content is specifically sexual or not, is perhaps the distinguishing contribution to privacy analysis of the First Amendment approach.

A First Amendment analysis of privacy teaches that an application of First Amendment guarantees exclusively to speakers will not adequately protect a free expression system; decision-makers must be sheltered, too. For the protection of privacy, the analysis yields a constitutional interest which cannot always be vindicated because it must compete with conflicting constitutional interests arising from the same logic. Yet it is the nature of privacy to be entangled with other social interests and values;[86] privacy in law cannot be less entangled with and compromised by other legal goals. The First Amendment analysis of privacy makes these entanglements and compromises explicit.

86. *See, e.g.*, Simmel, *supra* note 58.

Law School of Harvard University
Cambridge, Mass. 02138

July 9, 1974

Senator Sam J. Ervin
Chairman, Committee on
Government Operations
United States Senate
Washington, D. C. 20510

Dear Senator Ervin:

Your letter of June 25 concerning S. 3418 and related bills dealing with privacy arrived at a time when I am too heavily committed on other matters to undertake a detailed analysis of the proposed legislation. This I very much regret, since I am most interested in the subject matter.

I enclose a copy of an article on the subject which I published in the May, 1971, issue of the Texas Law Review. I regret that I cannot possibly do more at this time.

Sincerely,

Vern Countryman
Professor of Law

VC:bg

Enclosure

TEXAS LAW REVIEW

VOLUME 49 MAY 1971 NUMBER 5

Copyright 1971 By Texas Law Review, Inc.

THE DIMINISHING RIGHT OF PRIVACY: THE PERSONAL DOSSIER AND THE COMPUTER

VERN COUNTRYMAN*

Unreliability and abuse in data collection, and the irreducible danger of illegal access to the growing, computerized personal data files of private and public agencies, Professor Countryman argues, pose control problems that defy conventional regulation. He urges that preservation of privacy demands sweeping congressional reevaluation of society's need for such files and suggests that those not serving "an actual need for a vital public purpose" be done away with.

The compiling of dossiers on individuals is not new in this country. The Federalists doubtless compiled dossiers on real and suspected Jacobins during the enforcement of the first Alien and Sedition Acts. After the prosecutions of suspects were completed, however, or at least when the Alien and Sedition Acts were repealed, those dossiers were apparently discarded.

As our numbers have increased and our society grown more complex, we have recognized ever more reasons—political, social, and economic—why one man has a "legitimate" interest in the affairs of another. For example, a company that contemplates extending credit to, insuring or employing John Doe asserts a "legitimate" interest in knowing something about his economic condition and often some of his other characteristics also. Responding to this asserted interest, an entire industry has developed to supply the needed information. And, because it is not efficient for a new compilation to be initiated every

* Professor of Law, Harvard University; B.A., University of Washington, 1939; LL.B., University of Washington, 1942. This article is derived from the fourth annual Orgain Lecture, delivered at the University of Texas Law School in March, 1971.

The Will E. Orgain Lectureship was established by the family and friends of the late Mr. Orgain as an endowment fund through the University of Texas Law School Foundation. The annual lectureship consists of a single lecture on a subject related to law delivered by a distinguished scholar.

time a new need arises, this industry maintains permanent dossiers on each of its subjects—dossiers whose final entries probably reflect not the death of the subjects, but the closing of the probate of their estates. Law enforcement agencies also profess a "legitimate" interest in compiling dossiers on suspected law violators. Here again, efficiency is interposed as a justification for maintaining the dossiers even after the case is closed.

Since World War II it has become fashionable to utilize a variety of prophylactic measures both to identify potential criminals before crimes are committed and to frustrate supposed intentions of potential criminals. These efforts include various loyalty programs, a bewildering variety of laws defining sedition and other political crimes, and the antics of legislative committees. To meet the "legitimate need" for the protection of government, many government agencies have gone into the business of compiling dossiers on the political beliefs, expressions, and associations of all those characterized as "subversive." Here, too, it is more efficient that these dossiers be permanent.

But the demands of that outstanding of all American virtues—efficiency—do not end here. Just as it is efficient for any one dossier compiler to maintain a permanent record on each subject, it is inefficient for another compiler not to utilize previous compilations. The drive for efficiency has inexorably led to a considerable interchange of data between compilers both within the generous limits allowed by law and sometimes beyond those limits.

The computer has further facilitated the quest for efficiency. With its endless capacity to store data and to regurgitate it with lightning-like speed, it is inefficient not to use the computer to combine the various dossiers compiled on each individual. If the present trend continues, the day will come when the push of a button will produce a complete "data profile" on each citizen, from his departure from the womb (or perhaps sometime earlier) to some time after he enters his tomb. While we cannot yet predict the precise arrival of this glorious day, there is enough available information to indicate the actuality of this trend and to provoke every concerned citizen to demand more information about and more protection against this development.

I. Privately Compiled Dossiers

Within the private sector, the compilation of data on individuals is most frequently undertaken for profit, although the motivation is

occasionally punitive or benevolent. Since Congress in recent years has investigated the operation of commercial agencies,[1] we are most knowledgeable about them. These commercial agencies fall into two categories: the credit bureau and the investigatory reporting agency.

A. The Commercial Compilers

In a very rough way, the credit bureau is to the user of consumer credit what Dun & Bradstreet's reporting service is to a business organization seeking credit. The credit bureau is not a new institution in our society, but as consumer credit has burgeoned by more than 2,000% in the past quarter century[2] so has the business of the credit bureau.

There are approximately 2,500 credit bureaus in the country, of which some 2,100 are members of one trade association, Associated Credit Bureaus, Inc. The files of bureaus affiliated with ACB include records on approximately 100 million persons, and those bureaus interchange their information.[3] The largest credit bureau operation outside the ACB is the Credit Data Corporation, which has files on 27 million persons.[4] While there is doubtless some overlap between the 100 million ACB files and the 27 million Credit Data Corporation files, the combined accumulation probably covers nearly all 131 million of us who are over eighteen years of age, particularly since most of the

---

1 There have been five separate Congressional hearings: *Hearings on Commercial Credit Bureaus Before the Spec. Subcomm. on Invasion of Privacy of the House Comm. on Gov't Operations*, 90th Cong., 2d Sess. (March 1968) [hereinafter cited as *House Credit Bureau Hearings I*]; *Hearings on Retail Credit Co. of Atlanta Before the Spec. Subcomm. on Invasion of Privacy of the House Comm. on Gov't Operations*, 90th Cong., 2d Sess. (May 1968) [hereinafter cited as *House Credit Bureau Hearings II*]; *Hearings on S. Res. 233 Before the Subcomm. on Antitrust and Monopoly of the Senate Judiciary Comm.*, 90th Cong., 2d Sess. (December 1968) [hereinafter cited as *Senate Credit Bureau Hearings I*]; *Hearings on S. 823 Before the Subcomm. on Financial Institutions of the Senate Banking and Currency Comm.*, 91st Cong., 1st Sess. (May 1969) [hereinafter cited as *Senate Credit Bureau Hearings II*]; *Hearings on H.R. 16340 Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 2d Sess. (March-April 1970) [hereinafter cited as *House Credit Bureau Hearings III*].

2 From $5.7 billion at the end of 1945 to $123.9 billion at the end of November 1970. FED. RESERVE BULL. A-54 (Jan. 1971).

3 ACB is also operating under a 1933 antitrust consent decree that requires the interchange of data with the 4000 credit bureaus not affiliated with it. *See* United States v. National Retail Credit Ass'n, Eq. No. 10420 (E.D. Mont., Oct. 6, 1933) (abstracted in AM. ENTERPRISE INSTITUTE FOR PUB. POLICY RESEARCH, ANTITRUST CONSENT DECREES 1906-1966, at 371 (1968)); *Senate Credit Bureau Hearings I*, *supra* note 1, at 23. In 1968 ACB entered into arrangements with International Telephone & Telegraph Corporation to provide a computer service to facilitate the interchange. *Id.* at 24, 33-34.

4 In November 1969 all of the stock of Credit Data Corp. was acquired by TRW Credit Information Services, Inc., which now operates the Credit reporting service as TRW Credit Data. *House Credit Bureau Hearings III*, *supra* note 1, at 156. This bureau is completely computerized and is adding files at the rate of one-half million per month. *House Credit Bureau Hearings III*, *supra* note 1, at 157, 165; *Senate Credit Bureau Hearings II*, *supra* note 1, at 223, 227.

93 million of us who are married will be combined in some 46 million files with our spouses.[5]

The content and the reliability of information in credit bureau files is dictated largely by the three principal sources from which the credit bureaus draw. A principal source of information is the bureau's own subscribers, the merchants, banks and finance companies who buy most of the credit reports. They supply information on their own customers with regard to employment, approximate income and credit performance. The value of this source is subject to three significant limitations. First, since the credit bureau files do not reveal the subject's net worth, or even his state of solvency, but only whether his accounts with the bureau's subscribers are delinquent, the extension of credit in reliance on a credit bureau report proceeds on the illogical assumption that the ability to meet current credit payments betokens the capacity to handle one additional debt. Second, credit bureau files cannot even approximate the amount of a subject's debts, since many creditors are not subscribers. Third, the delinquency of an account frequently results not from financial irresponsibility but from a bona fide dispute over the amount owing or the quality of merchandise sold.

As a second source of information, the more enterprising bureaus scrutinize official records for arrests, lawsuits, judgments, bankruptcies, mortgages, tax liens, marriages, divorces, births and deaths. The substantial possibility of mistaken identity, combined with the frequent failure of official records to include final dispositions, renders this source highly unreliable. As a third source of information, most credit bureaus also maintain a news-clipping service, although this occasionally serves as a substitute for checking official records. Obviously, this source poses even greater danger of error than the official record check with regard to mistaken identity or the failure to note the ultimate disposition of arrests, lawsuits, judgments and liens.

During Congressional hearings on the subject, much attention was focused on the denial of credit due to erroneous adverse information in credit bureau files. Unstressed but equally serious is the erroneous extension of credit. Just as mistaken identity leads to the insertion of data in an inappropriate file, so also its leads to the omission of relevant information from the appropriate file. And few, if any, files will record all debts. Inaccurate files thus mean that credit is both erroneously denied and granted. In their own defense, credit bureaus

5 U.S. BUREAU OF THE CENSUS, STATISTICAL ABSTRACT OF THE UNITED STATES 25, 32 (1970).

stress that they only collate information and that they never claim to make affirmative investigations of their subjects.[6]

It is no coincidence that, as consumer credit expanded by more than 2,000% in the past twenty-five years, so did consumer bankruptcies—from 8,500 in 1946 to 178,000 in 1970.[7] If a credit extender were to compare the report he received from the credit bureau with the debts scheduled by a subject in his bankruptcy proceeding, he might conclude that the credit report was not worth the 35 to 75 cents paid for it.[8] Upon entries of such fragile reliability is your "credit rating" built. And when the credit bureaus also engage in debt collection—and many of them do, finding their ability to affect the credit rating an effective collection tool[9]— the reliability of the entries is even further threatened by a built-in conflict of interest.

Credit bureau files are thus inadequate to satisfy some who contemplate commercial relationships. In consequence, prospective employers and insurers often turn for information to the investigatory reporting agency.[10] Congressional committees heard from representatives of the largest of such agencies in this country—Retail Credit Company of Atlanta, with 1,225 offices, 7,000 inspectors, and files on 48 million persons.[11] Inspectors from Retail Credit not only check

---

[6] On occasion, however, bureaus join with local merchants in sponsoring the Welcome Wagon lady who reports back to the merchants on the apparent worldly needs of the newcomers she visits and to the credit bureau on their apparent credit worthiness—and on where the newcomer came from, so that his file can be obtained from a credit bureau at his former location. *Senate Credit Bureau Hearings II*, *supra* note 1, at 119, 167-172; *House Credit Bureau Hearings III*, *supra* note 1, at 33.

[7] AD. OFFICE OF UNITED STATES COURTS, TABLES OF BANKRUPCY STATISTICS, TABLE F-3 (1946); AD. OFFICE OF UNITED STATES COURTS, ANN. REP. OF THE DIRECTOR, V-4 (1970).

[8] This is the price the subscriber pays to learn what reposes in the compiler's file at the moment he makes inquiry. If he wants the file brought up to date by calls to other subscribers he must pay an additional fee. Save for routine checking of public records and newspaper clippings, the files are not updated until a subscriber requests, and pays for, that action.

In hearings held in Washington, D.C. in March, 1968, a New York Congressman asked for a demonstration of Credit Data Corporation's high-speed computerized retrieval of his New York City credit file. Within the time consumed by six pages of printed hearing record, the report came back on one bank loan as of June, 1967, and nothing else. The Congressman's response: "A very inefficient system, thank God." *House Credit Bureau Hearings I*, *supra* note 1, at 72-79.

[9] *Senate Credit Bureau Hearings I*, *supra* note 1, at 5, 23, 28-30, 40-43, 45, 53, 78; *Senate Credit Bureau Hearings II*, *supra* note 1, at 180.

[10] Two of the subcommittees also heard testimony from representatives of one agency specializing in reports on prospective mortgagors to banks and institutional lenders. Their testimony was to the effect that they confined their investigation to public records and newspaper clippings, did not engage in "questioning neighbors," and always gave the subject an opportunity to explain adverse items of public record or news report—unless the client asked them not to contact the subject or unless the client asked for a quick, telephone report on what the files contained. *Senate Credit Bureau Hearings II*, *supra* note 1, at 237-254; *House Credit Bureau Hearings III*, *supra* note 1, at 211-230.

[11] *Senate Credit Bureau Hearings II*, *supra* note 1, at 175; *House Credit Bureau Hearings III*, *supra* note 1, at 473-474.

public records and clip newspapers, but also interview friends, neighbors, former neighbors, acquaintances, employers, former employers, business associates—anyone who may know something, or have an opinion, about the subject.[12] For life insurance companies Retail Credit inspectors inquire about the subject's drinking habits and domestic difficulties, seek out criticism of his character and morals, and report whether his living conditions are crowded or dirty.[13] For automobile insurers Retail Credit investigates the subject's neighborhood business reputation, morals, and "antagonistic-antisocial conduct."[14] For employers, Retail Credit's inspectors also report whether the subject has any "known connection with a 'peace movement' or any other organization of a subversive type" and whether he is reputed to be "neurotic or psychotic."[15]

In response to Congressional concern about the reliability of agency reports, spokesmen for Retail Credit proffered two assurances. First, its inspectors are carefully trained persons of "unusual inspection ability."[16] This assurance lost some of its force when inquiry revealed that these highly qualified, well-trained inspectors commanded a starting salary of $475 to $500 per month, that they prepared anywhere from 2 to 16 reports per day, that half had no more than a high school education, and that another 30% were college dropouts.[17] Second, Retail Credit reported that adverse information not coming from public records either is confirmed from a second source or is reported as unconfirmed.[18] Whatever comfort otherwise might be drawn from this assurance is somewhat qualified by evidence to the contrary.[19]

---

12 *House Credit Bureau Hearings II, supra* note 1, at 21; *Senate Credit Bureau Hearings I, supra* note 1, at 108.

13 *Senate Credit Bureau Hearings II, supra* note 1, at 196-203.

14 The auto insurers are convinced that there is some correlation between all of these factors (except antagonistic-antisocial conduct) and accident frequency, and that both immorality and antagonistic-antisocial conduct would impair the subject's effectiveness as a witness in the event of litigation. *Senate Credit Bureau Hearings II, supra* note 1, at 207-212, 305-316; *House Credit Bureau Hearings III, supra* note 1, at 514-516. The latter consideration, of course, should dictate an inquiry into hare-lips, unsightly scars and birthmarks, and the use of deodorants.

15 *Senate Credit Bureau Hearings I, supra* note 1, at 109-110; *Senate Credit Bureau Hearings II, supra* note 1, at 176-177.

16 *House Credit Bureau Hearings II, supra* note 1, at 19-20; *see also Senate Credit Bureau Hearings II, supra* note 1, at 175-176.

17 *Senate Credit Bureau Hearings II, supra* note 1, at 176, 192; *House Credit Bureau Hearings III, supra* note 1, at 473, 503.

18 *House Credit Bureau Hearings II, supra* note 1, at 21; *House Credit Bureau Hearings III, supra* note 1 at 474.

19 One well-trained, highly-qualified inspector, who heard from two sources that a subject had served in prison, reported the prison record as an unqualified fact although the inspector found no confirmation in court or prison records. Wagner v. Retail Credit Co., 338 F.2d 598 (7th Cir. 1964).

Access to the files of these commercial compilers is reportedly restricted to "reputable" business organizations that possess a "legitimate" business interest.[20] However, Congressional and private inquiry has undercut this assertion and ably demonstrated the easy availability of the files, not only to private parties[21] but also to government agencies.[22]

---

20 *House Credit Bureau Hearings I, supra* note 1, at 63-64, 90; *House Credit Bureau Hearings II, supra* note 1, at 19; *Senate Credit Bureau Hearings I, supra* note 1, at 62.

21 Credit bureau spokesmen have admitted the possibility of an employee of a credit bureau subscriber obtaining a report for purposes unrelated to his employer's business. *House Credit Bureau Hearings I, supra* note 1, at 111; *Senate Credit Bureau Hearings II, supra* note 1, at 228. Retail Credit's spokesmen admitted that it sometimes gave out reports as a "favor" when, for example, an executive of a subscriber asked for a report on a man being considered as a new minister for his church. *House Credit Bureau Hearings II, supra* note 1, at 19, 38; *Senate Credit Bureau Hearings I, supra* note 1, at 101.

Moreover, the compilers had been under interrogation by Congressional committees for over a year when CBS News conducted an experiment. Using a fictitious company name, it sent out twenty letters to credit bureaus requesting reports on named individuals. It received ten reports and offers of two more if it would sign a subscriber's contract. On a second effort, the fictitious company sent out twenty-eight letters. This time it did not state that it was considering granting credit—it simply asked for a full credit report, without stating why it wanted it. And this time it asked only about individuals who had been complaining to Congressional committees about the credit bureaus. This time it received only seven of the requested reports—plus one more when it accepted the offer of one credit bureau to sign a subscriber's contract. *Senate Credit Bureau Hearings II, supra* note 1, at 378-381; *House Credit Bureau Hearings III, supra* note 1, at 59-61.

22 This includes not only such governmental credit-granting agencies as the Federal Housing Administration and the Veterans Administration, which buy such reports just as do private subscribers. It includes also such law enforcement agencies as the FBI and the Internal Revenue Service. Members of ACB and the Retail Credit Company make their files available to the law-enforcers "as a public service." *House Credit Bureau Hearings I, supra* note 1, at 134-138; *House Credit Bureau Hearings II, supra* note 1, at 23, 39; *Senate Credit Bureau Hearings II, supra* note 1, at 149, 161; *House Credit Bureau Hearings III, supra* note 1, at 603, 605. The Credit Data Corporation took a different view, and refused to turn over its reports to the IRS. *House Credit Bureau Hearings I, supra* note 1, at 90-91; *Senate Credit Bureau Hearings I, supra* note 1, at 62-63. It was then met with a statutory summons calling for all credit information relative to named taxpayers. The IRS is authorized, for the purposes of "determining the liability of any person for any internal revenue tax" to summon the taxpayer "or any other person the [IRS] may deem proper," to produce "such books, papers, records, or other data . . . as may be relevant or material to such inquiry . . . ." INT. REV. CODE OF 1954, § 7602. When Credit Data refused to obey the summons, IRS got a judicial order of enforcement pursuant to the statute, requiring it to comply on payment by the IRS of 75 cents per report, the fee which Credit Data charged its regular subscribers. On appeal, Credit Data won a great victory. The decision below was affirmed in all respects save that the case was remanded to determine the "fair value" which IRS must pay for the reports—the rate paid by subscribers was not to be taken as conclusive because subscribers supply "valuable credit information" to Credit Data. United States v. Davey, 426 F.2d 842, 844 (2d Cir. 1970).

The result was foreshadowed by previous decisions of the Supreme Court. In a long line of cases that court has sustained judicial enforcement of an administrative agency's statutory subpoenas against fourth amendment attack where the subpoena sought testimony about the affairs or the records of the person subpoenaed, if the subpoena was sufficiently specific to satisfy the fourth amendment, if the administrative inquiry was authorized by Congress, and if the evidence sought was relevant to the inquiry—the court's application of the last two requirements when its enforcement order was sought being held to satisfy the fourth amendment's requirement of probable cause. United States v. Morton Salt Co., 338 U.S. 632 (1950); Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186 (1946). Earlier decisions are discussed in 1 K. DAVIS, ADMINISTRATIVE LAW TREATISE § 3.12 (1958) and Comment, *Agency Access to Credit Bureau Files: Federal Invasion of Privacy?* 12 B.C. IND. & COM. L. REV. 110, 113-118 (1970). More than forty-five years ago the Supreme Court also

Notwithstanding the otherwise easy accessibility of files, commercial compilers steadfastly refuse to permit the subject to see the file. Three reasons are given for this position—one laughable and two believable. First, if the subject ever got his hands on the file, even in the compiler's office, he might destroy it. Second, to let the subject see the file would be to reveal the compiler's sources and would tend to "dry up" those sources.[23] Third, if the file consists of a computer printout, the subject wouldn't be able to understand it.[24]

As a consequence of past practices, many subjects do not know that a denial of credit, employment or insurance may be caused by an adverse report from a commercial compiler. Even the individual who is aware of that fact, and who believes that the adverse report is erroneous, seldom can obtain legal relief. If he sues on a theory of defamation or interference with economic expectations, he encounters the defense of qualified privilege: the subscriber's "legitimate" interest in the subject's affairs protects the compiler who avoids gross negligence or malice.[25] If the subject resorts to an action for invasion of privacy, he confronts the traditional assertion[26] that the right to privacy proscribes only *publicizing* private matters. Even if he persuades a court

---

summarily affirmed a decision that no fourth amendment question was even presented when the IRS, investigating the tax liability of a bank depositor, summoned the bank to produce its records. First National Bank of Mobile v. United States, 267 U.S. 576 (1925). Since the Credit Data case was decided, the Supreme Court has unanimously extended that ruling to cover an IRS summons to the taxpayer's employer and, by dictum, to any other third person with no established legal privilege, such as an attorney, where the taxpayer has "no proprietary interest of any kind" in the records subpoenaed. *See* Donaldson v. United States, 91 S. Ct. 534, 538 (1971) (taxpayer sought to intervene in the enforcement proceeding against the employer, but was held not to have a sufficient interest to entitle him to do so.); *cf.* Reisman v. Caplin, 375 U.S. 440 (1964). The fourth amendment, therefore, offers no apparent protection to the subject whose file in a credit bureau is subjected to an administrative subpoena or summons of a governmental agency showing a "legitimate" interest in its contents.

23 Doubtless this reason should be expanded to say that the nondisclosure of the files protects not only the compiler's sources, but also the compiler himself from trouble (including litigation) with the subject.

24 *See House Credit Bureau Hearings I, supra* note 1, at 97; *House Credit Bureau Hearings II, supra* note 1, at 13-16; *Senate Credit Bureau Hearings I, supra* note 1, at 21-22, 114-115; *Senate Credit Bureau Hearings II, supra* note 1, at 153, 173, 179, 232-233, 270; *House Credit Bureau Hearings III, supra* note 1, at 160, 168, 460-461, 466-467, 490.

25 *See* Roemer v. Retail Credit Co., 3 Cal. App. 3d 368, 83 Cal. Reptr. 540 (1970); Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 345-347 (1966); Comment, *Credit Investigations and The Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509, 513-523 (1959). The first amendment protection accorded defamatory but nonmalicious news stories about public figures by New York Times Co. v. Sullivan, 376 U.S. 254 (1964), has been held not to extend to private subscription credit reports. Grove v. Dun & Bradstreet, Inc., 438 F.2d 433 (3d Cir. 1971).

26 For the famous law review article that launched this concept into American jurisprudence see Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *See also* Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326 (1966).

that the concept has developed to protect against all offensive intrusions into private affairs,[27] the court may respond that this right is qualified by the "legitimate" interest of the user of the files.[28]

Notwithstanding this lack of judicial empathy, Congressional investigators were sympathetic to individuals whose dossiers contained erroneous adverse information. The result was enactment[29] of the Fair Credit Reporting Act of 1970.[30] The Act applies only to the accuracy and accessibility of the reports. No attempt is made to limit the nature of their contents. The report which the Act reaches, whether issued by

---

27 *See* 1 F. HARPER & F. JAMES, THE LAW OF TORTS § 9.6 (1956); W. PROSSER, THE LAW OF TORTS § 112 (3d ed. 1964).

28 Shorter v. Retail Credit Co., 251 F. Supp. 329 (D.S.C. 1966); Comment, *Credit Investigations and The Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509, 523-527 (1969).

29 The compilers detected this Congressional sentiment and decided that if they could not fight the move for reform, they had better join the effort in hope of obtaining a palatable result. *See* Denney, *Federal Fair Credit Reporting Act*, 25 PERS. FIN. LAW Q. REP. 4 (1970). *See also House Credit Bureau Hearings III*, *supra* note 1, at 108.

30 84 Stat. 1114, tit. VI (1970 U.S. CODE CONG. & AD. NEWS 5142). This Act, applicable both to credit bureaus and to investigatory reporting agencies, attempts to guard against inaccurate or stale information in their reports and to restrict the use of the reports by provisions that:

(1) Require the compilers to maintain "reasonable procedures" to eliminate from their reports bankruptcies after 14 years and other adverse information after 7 years.

(2) Require the employers to keep their public record entries in employment reports up to date to the extent that the public records are up to date, and require the investigatory agencies to confirm their adverse interview information at least 3 months before reporting it.

(3) Require users of investigatory reports to notify the subject that such a report is being made; require users of credit or investigatory reports to advise the subject whenever credit, insurance or employment is denied, "wholly or partly because of" the report and to identify the reporting agency; and require compilers reporting adverse public record information for employment purposes to advise the subject of that fact.

(4) Require any compiler, on request of a subject, to disclose to him the "nature and substance" of the information on him in its files (but not the file itself); require credit bureau compilers to disclose also the sources of their data; and require all compilers to reinvestigate any item which the subject disputes and, if it does not correct the item, to include in future reports his statement of not more than 100 words describing the dispute unless the compiler has "reasonable grounds to believe" the statement is "frivolous or irrelevant."

(5) Require the compilers to maintain "reasonable procedures" to confine the furnishing of their reports, without written consent of the subject, to those who have "a legitimate business need" for them.

(6) Forbid compilers, without written consent of the subject, to furnish more than name, address and place of employment of a subject to a governmental agency except in connection with licensing, governmental grants or other business transactions where the government has a "legitimate business need"—and except in response to court order.

(7) Authorize damage actions for subjects when there is negligence in failing to comply with the Act, punitive damages for wilful noncompliance with the Act, and administrative enforcement by the FTC.

(8) Immunize compilers and their sources of information from any other liability save for false information "furnished with malice or wilful intent to injure" the subject.

(9) Impose criminal penalties for officers or employees of compilers who "knowingly and wilfully" make unauthorized disclosures of information and for any person who "knowingly and wilfully" obtains such information "under false pretenses."

a credit bureau or an investigatory agency, is defined to mean any communication bearing not only on credit, but also on "character, general reputation, personal characteristics, or mode of living."

B. The Punitive Compilers

There has been no official investigation of those private compilers who assemble dossiers for the purpose of punishing those with whom they disagree. Nonetheless, it is safe to generalize that the punitive compilers are sponsored and staffed by right-wing extremists. This is not to say that right-wing extremists are more (or less, depending upon your point of view) lacking in virtue than left-wing extremists. The explanation derives from the fact that official investigations of extremist groups have almost invariably focused on those on the left end of the political spectrum (although they tend to hit anyone to the left of the right-wing extremists). Hence, since private punitive compilers rely almost entirely upon official investigations as their sources of information, there is not enough available information to compile dossiers on right-wing extremists. Moreover, in the absence of official investigations to whet the public interest, there would be no substantial market for dossiers on right-wing extremists even if they could be compiled.

Some punitive compilers, like American Business Consultants, operate for profit. Organized by three former FBI agents, this group operated during the heyday of Senator Joseph McCarthy. It published the newsletter *Counterattack*, which provided dossiers on those not sufficiently anti-Communist, with special emphasis on the news media, writers and publishers, and *Red Channels*, which focussed on those similarly lacking in the entertainment business.[31] Other punitive compilers, like the Americanism Committees of some American Legion posts, the John Birch Society, and Aware, Inc. operate out of their own versions of patriotism.

The punitive compilers' principal aim is to deprive the subject of his employment. Since their dossiers are neither solicited nor often wanted by employers, the "legitimate" needs of the employer cannot be justifiably invoked as a defense to a defamation or an invasion of privacy action. Offsetting their apparent legal vulnerability is the fact that most, if not all, of the punitive compilers are either completely

---

[31] *See* M. MILLER, The JUDGES AND THE JUDGED (1952).

judgment proof or incapable of responding in damages for the full injury caused.[32]

C. *The Benevolent Compilers*

Many of those who compile personal dossiers, or who support their compilation, are interested not in the individual subjects but in groups. Included in this category are the government officials and business executives who seek to make informed decisions and plans, and the scholars (particularly the social scientists) who seek to aid decision making and planning. Although the interest is confined to groups, it is inescapable that information about groups must come from, and relate to, individuals.

At first blush it might seem that group information could be obtained and compiled without preserving a record of the identity of the component individuals. Unfortunately, some key to the identity of the subjects must be retained if group compilations are to be kept current and if the compilations are to be available for new uses. So long as keys to the identity of those in the group are retained, these compilations provide a potential source of personal dossiers, either as a consequence of unauthorized use or as a consequence of a change in the policy of the compilers. Unfortunately, many of those who use group compilations are so single-mindedly devoted to their own purposes that they are heedless of this danger. Thus, a committee of the Social Science Research Council in 1965 proposed that the Bureau

---

32 Both of these facts were dramatically demonstrated by a distinguished and courageous graduate of the University of Texas, John Henry Faulk. He lost his position with CBS in 1956 as a consequence of a publication of a dossier—largely based on erroneous information in the files of the House Un-American Activities Committee—in a bulletin published by Aware, Inc. In part, also, the loss of his job was due to an advertising boycott launched by the owner of a chain of grocery supermarkets after the bulletin was published. Faulk sued Aware, one of its employees and the supermarket owner for libel, realizing that Aware and its employee were not capable of responding in damages in any sufficient amount. After a trial in which the court ruled that the defense of qualified privilege was not available and that defendants had failed to prove the defense of truth, the jury returned a verdict for $3,500,000—of which $1,000,000 was actual damages against all three defendants, $1,250,000 was punitive damages against Aware, and $1,250,000 was punitive damages against its employee. There was no award of punitive damages against the supermarket owner because, unfortunately, he died shortly before the case went to the jury. The judgment against him was settled with his disappointingly small estate for $175,000. After an appeal by the surviving defendants in which they were castigated as "malicious" and "vicious" purveyors of libel, the judgment was reduced to $400,000 total actual damages, $50,000 punitive damages against Aware and $100,000 punitive damages against its employee, no part of which was collectible from Aware or its employee. Faulk v. Aware, Inc. 19 App. Div. 2d 464, 244 N.Y.S.2d 259 (1963), *aff'd*, 14 N.Y.S.2d 899, 200 N.E.2d 778, 252 N.Y.S.2d 95 (1964), *cert. denied*, 380 U.S. 916 (1965). *See also* J. FAULK, FEAR ON TRIAL (1964). Faulk's attorney has also written about the case in his usual self-effacing manner. *See* L. NIZER, THE JURY RETURNS 225-438 (1966). Neither book reveals how much of the $175,000 actually collected went to Faulk.

of the Budget establish a National Data Center to collect and computerize all machine-readable data of all federal agencies for use both by the government and by individual scholars. The report was eloquent on the "efficiency" of such an operation, but took account of the threat to individual privacy only to the extent of suggesting that when a government agency has obtained data under a pledge of confidentiality, "it is often possible to disguise the information in such a way that specific data cannot be traced to any individual respondent."[83]

A personal experience provides another illustration of the scholar's insensitivity to problems of privacy where his thirst for knowledge is concerned. Early in 1969, a private foundation sent out a questionnaire to university graduate students seeking their opinions on a variety of subjects ranging from drug use to forcible overthrow of the government. Since the students were instructed to return these questionnairses with their names on them, one graduate student called me to ask if there was any danger, despite the foundation's assurance of confidentiality, that his replies might come into the hands of a government agency. My advice, subsequently printed in the *Harvard Crimson*, was that the foundation would have no defense to an administrative or legislative subpoena. I thereupon received a lengthy letter from a Harvard professor of government taking me to task. First, he explained to me that he had nothing to do with the particular questionnaire but assured me, based on his thirty-five years of experience, that it was "typical of those used by both academic and commercial pollsters." Second, he explained to me—not quite as adequately as I have explained to you—why the identity of those polled must be preserved. Third, he expressed doubt that any government agency would seek to obtain the information. Fourth, though he was not a lawyer, he ventured the opinion that the courts would very likely create some sort of

[83] The report is printed in *Hearings on the Computer and Invasion of Privacy Before the Spec. Subcomm. on Invasion of Privacy of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess., ser. 1, pt. 1, at 195, 202.

The Bureau referred the report for review to a research analyst employed by Resources for the Future, Inc., a private foundation. He endorsed the proposal in a report much concerned with organizational and operational problems but which did not mention problems of privacy. *Id.* at 254. The Bureau next created a task force, consisting of one statistician and five academicians, to consider the problem. The task force also endorsed the proposed National Data Center, but its report took account of hearings on the subject wherein congressmen had been highly critical of the danger to privacy. The task force took this criticism rather lightly, however, since it thought that Congress could define a standard for access to the data in the center that could be enforced and that the technical possibility that the federal computers might themselves be tapped by technological means could be met by unspecified "organizational and technical means . . . available to control and limit the risks." This report is printed in *Hearings on S. Res. 25 on Computer Privacy Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 90th Cong., 1st Sess., ser. 1, pt. 1, at 25, 37 (1967).

privilege to block a government subpoena. Fifth, he pointed out that advice such as mine might well reduce the number of responses to the questionnaire. Finally, he urged me to reconsider and to issue another statement on the matter. I declined his invitation on the grounds that I thought my legal advice was better than his and that the students were entitled to have that advice so that they, rather than he, I, or the foundation, could do their own speculating about the likelihood of a government subpoena.

This is not to suggest that all group compilers are insensitive to the privacy problem or to the danger that the compilations might provide a source for personal dossiers. But, even awareness of this danger betokens only the intention, not the ability, to safeguard the compilations. Once the data has been amassed, even the best intentioned compiler can do little more than attempt to guard the identity of subjects and hope that his successors in control of the compilation will be similarly sensitive to the danger.[34]

II. Publicly Compiled Dossiers

If information on private compilers of dossiers is incomplete, the information available on governmental compilers is fragmentary. The little that is known is based on disclosures made by the news media and on sporadic hearings conducted by Senate subcommittees.

Since the government can compel the subject to provide information about himself, the government has a unique source of information. In addition, governmental compilers also rely, as does the Retail Credit Company, on the personal interviewing of neighbors, associates, and acquaintances of the subject. Although government investigators are better paid, and hopefully better qualified and trained, than private inspectors, the difference may not be enough to inspire great confidence in the objectivity of their work product.[35]

---

[34] The problem is well illustrated by the United Planing Organization (UPO) of Washington, D.C., a private organization devoted to combatting problems of poverty. In the course of its work, UPO has found it useful to compile data from public records on such matters as juvenile arrests, school dropouts, evictions and welfare payments. To guard the identity of its subjects, UPO transferred all of its data to a trustee under an irrevocable trust with strictures which permit UPO to have continued access to it only so long as it does not reveal the identity of its subjects. *Hearings on S. Res. 25 on Computer Privacy Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 90th Cong., 2d Sess., ser. 16, pt. 2, at 309-317 (1968). Under the terms of the trust, UPO apparently will indeed lose access to the data if it changes its policy and discloses the identity of its subjects or, possibly, if one of its officers or employees makes an unauthorized disclosure. But, by that time, personal dossiers on all of its subjects may be in someone else's computer.

[35] Those in academic life are familiar with the FBI agent and the military investigator who comes to inquire about former students seeking government employment or a military commission. Most would agree that there is no faster way to get the visitor out of the

A. Government's Power—Legal and Otherwise

Governmental compilers have another source of information disclaimed by Retail Credit Company: wiretapping and electronic bugging.[36] Because of what it reveals, with regard both to governmental attitudes toward individual privacy and to the feasibility of legislative efforts to protect privacy, it will be instructive to survey briefly the history of the use of these devices.

In 1928 the Supreme Court held that government wiretapping did not violate the fourth amendment.[37] In the Communications Act of 1934 Congress made it a crime for anyone, without authority of the sender, wilfully to intercept any communication by wire or radio and to divulge the contents of the intercepted communication to any other person.[38] Thereafter, the Court held that because a wiretap was illegal, evidence so obtained,[39] including the "fruit of the poisonous tree,"[40] was inadmissible in federal courts. Despite the clear holding that federal agents commit a federal crime when they tap telephones, the FBI has, with Presidential approval, continued to engage in wiretapping.[41]

---

office than to make clear that you have nothing derogatory to say about the subject. And I can testify from my own experience that the visitor will depart almost as rapidly if, in a case where you have something to say which might conceivably be considered derogatory, you tell the visitor you want your secretary to take down your statement so that you can send a copy to the subject.

[36] Spokesmen for Retail Credit Co. emphatically and repeatedly deny resorting to such methods. *See House Credit Bureau Hearings II*, *supra* note 1, at 16; *Senate Credit Bureau Hearings I*, *supra* note 1, at 101; *Senate Credit Bureau Hearings II*, *supra* note 1, at 180; *House Credit Bureau Hearings III*, *supra* note 1, at 473.

[37] Olmstead v. United States, 277 U.S. 438 (1928).

[38] 47 U.S.C. §§ 501, 605 (1964).

[39] Nardone v. United States, 302 U.S. 379 (1937). *See also* Weiss v. United States, 308 U.S. 321 (1939).

[40] Nardone v. United States, 308 U.S. 338 (1939).

[41] The FBI commenced the practice in 1931 and continued until March 1940, when Attorney General Jackson ordered it stopped, admitting that it was illegal. Brownell, *The Public Security and Wire Tapping*, 39 CORN. L.Q. 195, 197-199 (1954). Emerson & Haber, *Reply by the Authors*, 58 YALE L.J. 412, 414-415 (1949). In May 1940, however, President Roosevelt issued a secret directive, the existence of which was not made public until after his death, ordering wiretapping resumed against "persons suspected of subversive activities against the Government of the United States, including suspected spies." Brief of the United States at Appendix A, United States v. Dellinger, No. 69CR180 (N.D. Ill., Feb. 20, 1970); Theoharis & Meyers, *The "National Security" Justification for Electronic Eavesdropping: An Elusive Exception*, 14 WAYNE L. REV. 749, 759 (1968); Rogers, *The Case for Wire Tapping*, 63 YALE L.J. 793, 795 (1954); *Rejoinder by Mr. Hoover*, 58 YALE L.J. 422, 423 (1949). Thereafter, Attorney General Biddle in 1941 announced that the Department of Justice intended to use wire tapping in "espionage, sabotage, and kidnapping cases when the circumstances warranted," and President Truman in 1947 approved the use of wire tapping "in cases vitally affecting the domestic security, or where human life is in jeopardy." Brief of United States at Appendix B, United States v. Dellinger, No. 69CR180 (N.D. Ill. Feb. 20, 1970); Rogers, *supra* at 798. In 1964 President Johnson issued a directive forbidding wire tapping by federal agents, except in national security cases. And in 1965 Attorney General Katzenbach testified that, "under present law, [wire tapping] should be permitted only where national security is involved" and acknowledged that the department had 62 wiretaps then

The practice of electronic bugging has been governed by a series of decisions holding that the fourth amendment is not violated by the interception of communications by means of detectaphones or informers wired for sound, so long as the interception is accomplished without a physical trespass.[42]

Regardless of the state of the law or of the current content of executive directives, FBI Director Hoover has annually since 1965 assured the House Appropriations Committee that every wiretap undertaken by the FBI has been "approved in advance and in writing by the Attorney General" and that all taps were limited to "national security" or "internal security" cases.[43] But less than two months after he gave that testimony in 1969 an FBI agent testified in the trial of Cassius Clay that the FBI had tapped the wires of Martin Luther King for four years before his death in 1968.[44] Hoover then produced his version of an "approval in writing in advance by the Attorney General" —a memorandum written by one of Hoover's own subordinates, reciting that in 1963 Attorney General Robert Kennedy, now also deceased, had inquired "if it was feasible to use electronic devices" to

---

in effect "under my specific direction." *Hearings on S. Res. 39 on Invasion of Privacy (Gov't Agencies) Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Committee*, 89th Cong., 1st Sess., ser. 38, pt. 3, at 1155, 1641 (1965). In 1967 Attorney General Ramsey Clark issued a memorandum requiring prior written approval of the Attorney General for any federal wiretap or electronic bugging save in "national security" cases, which "shall continue to be taken up directly with the Attorney General in the light of existing stringent restrictions." Theoharis & Meyers, *supra* at 755-756. Since the Communications Act contains no exceptions, it is quite clear that the Department of Justice has been violating that Act for most of the time since its enactment. From time to time spokesmen for the Department have made the argument that the contents of wiretaps are not "divulged"—and hence the Communications Act is not violated—where the contents are merely communicated from one federal agent to another. Katzenbach, *An Approach to the Problems of Wiretapping*, 32 F.R.D. 107 (1963); Brownell, *supra* at 198. But this proposition has never been tested in the courts—the Department of Justice has never seen fit to prosecute an FBI agent or any other federal agent for violation of the Communications Act, even in cases where convictions of others have been reversed because the contents of wiretaps were divulged in court.

[42] Osborn v. United States, 385 U.S. 323 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952); Goldman v. United States, 316 U.S. 129 (1942); *cf.* Silverman v. United States, 365 U.S. 505 (1960) (use of "spike mike" in party wall held a forbidden physical trespass).

[43] *Hearings on Dep't of Justice Appropriations for 1970 Before a Subcomm. of the House Comm. on Appropriations*, 91st Cong., 1st Sess., 544 (1969); *Hearings on Dep't of Justice Appropriations for 1969 Before a Subcomm. of the House Comm. on Appropriations*, 90th Cong., 2d Sess., 549 (1968); *Hearings on Dep't of Justice Appropriations for 1968 Before a Subcomm. of the House Comm. on Appropriations*, 90th Cong., 1st Sess., 626 (1967); *Hearings on Dep't of Justice Appropriations for 1967 Before a Subcomm. of the House Comm. on Appropriations*, 89th Cong., 2d Sess., 262 (1966); *Hearings on Dep't of Justice Appropriations for 1966 Before a Subcomm. of the House Comm. on Appropriations*, 89th Cong., 1st Sess., 323 (1965).

[44] N.Y. Times, June 5, 1969, at 27, col. 1. *See also* United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *cert. granted*, 91 S. Ct. 457 (1971). Later testimony in the same trial revealed that the FBI had also tapped the wires of Black Muslim leader Elijah Muhammad from 1962 until 1966. N.Y. Times, June 8, 1969, at 29, col. 1.

check into allegations that King "had Marxist leanings."[45] The House Appropriations Committee found no reason to question Hoover's credibility when he appeared before it the following year and again testified that "all" wiretaps "were authorized in advance in writing by the Attorney General."[46]

Meanwhile, both constitutional and statutory requirements applicable to wiretapping and electronic bugging had changed. In 1967 the Court in *Berger v. New York*[47] invalidated a New York statute that authorized electronic bugging with prior court approval when physical trespass was involved, because the statute did not satisfy the fourth amendment's requirements[48] of specificity as to the crime involved or the conversations to be overheard. Later in the same year, in *Katz v. United States*,[49] the Court concluded that the fourth amendment applied both to wiretapping and to electronic bugging, regardless of physical trespass, thus requiring prior court approval for employment of either device under a procedure which would satisfy the specificity requirements of *Berger*.

In the Omnibus Crime Control and Safe Streets Act of 1968[50] Congress amended the Communications Act of 1934[51] so that its prohibition of interception and divulgence of communications is confined to radio communications, and established a procedure for judicial approval of wiretapping and electronic bugging that arguably does not meet the requirements of the *Berger* case.[52] That act also contains the following remarkable provision:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation . . . against foreign intelligence activities. . . . [or] limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by

45 N.Y. Times, June 21, 1969, at 11, col. 1.

46 *Hearings on Dep't of Justice Appropriations for 1971 Before a Subcomm. of the House Comm. on Appropriations*, 91st Cong., 2d Sess., 754 (1970) [hereinafter cited as *1971 FBI Appropriations Hearings*].

47 388 U.S. 41 (1967).

48 The fourth amendment was held applicable to the states in Wolf v. Colorado, 338 U.S. 25 (1949), and to require the exclusion in state courts of products of an illegal search in Mapp v. Ohio, 367 U.S. 643 (1961).

49 389 U.S. 347 (1967). Since these remarks were written, the use of the informer wired for sound, earlier approved in On Lee v. United States, 343 U.S. 747 (1952), has been resuscitated. United States v. White, 91 S.Ct. 1122 (1971).

50 18 U.S.C. §§ 2510-20 (Supp. V, 1970).

51 47 U.S.C. §§ 501, 605 (1964).

52 *See* Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 MICH. L. REV. 455, 460-477 (1969).

> force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.[53]

Whatever else this provision may do, it has emboldened Attorney General Mitchell to make the argument that the President has "inherent power . . . derived from the Constitution itself," free from judicial review under the fourth amendment, to employ wiretaps and electronic bugs "to gather foreign intelligence information" and "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to use unlawful means to attack and subvert the existing structure of the government."[54] This argument was first made and accepted by Judge Julius Hoffman in a case where the domestic threat to the "structure of the government" consisted of the disturbances at the Democratic National Convention in Chicago in 1968.[55] It has been rejected by the United States Court of Appeals for the Sixth Circuit and by a federal district court in California.[56]

B. The Compiling Federal Agencies

So much for sources.[57] What of the official dossiers compiled from these sources? Starting with the proposition that it is probably

---

53 18 U.S.C. § 2511(3) (Supp. V, 1970).

54 Brief for United States at 9, United States v. Dellinger, No. 69CR180 (N.D. Ill., Feb. 20, 1970) (Chicago Conspiracy Trial).

55 United States v. Dellinger, No. 69CR180 (N.D. Ill., Feb. 20, 1970). The government's argument as to foreign intelligence information was accepted in United States v. Brown, 317 F. Supp. 531 (E.D. La. 1970). *Cf.* United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *cert. granted*, 91 S.Ct. 457 (1971); United States v. Stone, 305 F. Supp. 75 (D.D.C. 1969).

56 United States v. Sinclair, 321 F. Supp. 1074 (E.D. Mich. 1971), *petition for mandamus denied sub nom.* United States v. United States Dist. Ct., Civ. No. 71-1105 (6th Cir., Apr. 8, 1971); United States v. Smith, 321 F. Supp. 424 (C.D. Cal. 1971). By separate concurring opinions in Katz v. United States, 389 U.S. 347 (1967), Justice White has approved and Justices Douglas and Black have rejected the notion that the government is not subject to judicial review under the fourth amendment in "national security" cases.

The Omnibus Crime Control and Safe Streets Act also requires annual reports to Congress of all court-approved wiretaps and bugs under the Act obtained by either federal or state authorities. 18 U.S.C. § 2519 (Supp. V, 1970). For the first full year of operation under the Act in 1969 these reports revealed 30 federal interceptions and 241 state interceptions, 176 of the latter being in New York alone. AD. OFFICE OF UNITED STATES COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS, Table I (1969). For the second year there were court authorizations for 183 federal interceptions and 414 state interceptions, including 215 by New York and 132 by New Jersey. N.Y. Times, May 3, 1971, at 1, col. 4. But the federal figures do not reveal all federal wiretaps because the federal government is acting on Attorney General Mitchell's contention that no court approval is required for tapping and bugging in "national security" cases. On a single day in March 1970, the FBI alone had 36 wiretaps and 2 bugs operating in cases so classified. *1971 FBI Appropriations Hearings, supra* note 46, at 754.

57 The governmental compilers also have another source of information not available to private compilers—the "mail cover" provided by the Post Office department. *See* 39

quite literally true that God only knows what is contained in the files of the CIA, some information is available about the files of some of the more obvious compilers.

1. FBI.—There has never been an official investigation of the FBI. Congressional committees occasionally hear something *about* the FBI, but, save J. Edgar Hoover's annual appearances before appropriations committees, Congress never hears *from* the FBI.[58] From Hoover's appearances we are advised that the FBI's computerized National Crime Information Center, which is tied to 24 computerized terminals throughout the country, contains in excess of 1.7 million personal files and contains also more than 195 million sets of fingerprints. The latter collection (with a substantial assist from state police forces and the Selective Service System and a lesser one from the tourists visiting the FBI headquarters who are persuaded to leave their fingerprints) is increasing at the rate of about 7 million per year.[59] Even with some allowance for foreigners, coverage must be approaching 100% of the adult population of the United States.

We can only speculate about the contents of the 1.7 million files. They are not disclosed to the public except as Hoover sees fit to reveal their contents in a book, an article or a speech.[60] But we can be sure that they are not confined to information related to enforcing the criminal laws. Since 1947 the FBI has been investigating federal em-

---

C.F.R. § 113.7 (1970). This source provides the name and address of the sender of mail to a suspect and, if desired, a facsimile of the sender's handwriting. *Hearings on Invasion of Privacy (Gov't Agencies) Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 89th Cong., 1st Sess., pt. 1, at 67, 117-120 (1965). The Post Office provides this service on request of any federal or state law enforcement agency, and averages about 1,000 mail covers per month. *Id.* at 68, 75, 83, 88, 93-94. One of the chief users of the service is the Internal Revenue Service, but both it and the Post Office declined to supply Congressional investigators with the names of those subjected to such surveillance, not only because some were still under investigation but also because such disclosure would constitute an invasion of the privacy of those investigated and found innocent of tax violations! *Id.* at 78, 97, 216. Although not specifically authorized by statute, the Post Office finds authority for the practice in its general statutory power to prescribe rules and superintend the business of the department. *Id.* at 68; *see* 39 U.S.C. § 501 (1964). Furthermore, the practice survived a challenge that it violated provisions of the criminal code forbidding delay of the mails. United States v. Costello, 255 F.2d 876 (2d Cir. 1958), *cert. denied*, 357 U.S. 937 (1958). *See also*, United States v. Schwartz, 283 F.2d 107 (3rd Cir. 1960), *cert. denied*, 364 U.S. 942 (1961).

[58] The authors of private studies of the FBI, which are now numerically balanced for [H. OVERSTREET & B. OVERSTREET, THE FBI IN OUR OPEN SOCIETY (1969); D. WHITEHEAD, THE FBI STORY (1956)] and against [F. COOK, THE FBI NOBODY KNOWS (1964); M. LOWENTHAL, THE FEDERAL BUREAU OF INVESTIGATION (1950)], were able to learn little about FBI files.

[59] *1971 FBI Appropriations Hearings, supra* note 46, at 692, 694, 712, 714. The problems confronting one who seeks to compel the FBI to remove from its files his fingerprints and notations covering his arrest and release without charge by state police were suggested but not resolved in Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970).

[60] *See, e.g.*, J. HOOVER, J. EDGAR HOOVER ON COMMUNISM (1969); J. HOOVER, A STUDY OF COMMUNISM (1962); J. HOOVER, MASTERS OF DECEIT (1958).

ployees and applicants for federal employment under the Federal Loyalty-Security Program, and since that time the Program has expanded to cover the employees of those who contract with various agencies and departments of the government. Investigations under that program delve even more deeply into the morality, beliefs and associations of the subjects than do the investigations conducted for private employers and insurance companies.[61]

If this were the extent of FBI surveillance, most of us who have never worked for, or sought to work for, the executive branch of the federal government or its contractors, and who have never done anything which would be likely to make us suspects of a federal crime (including the burgeoning list of political crimes), might be tempted to rest easy. But that is not all. Under the Emergency Detention Act of 1950[62] the President is authorized to declare an "Internal Security Emergency" in the event of invasion, declaration of war or "[i]nsurrection within the United States in aid of a foreign enemy." In that event, the Attorney General is to apprehend and incarcerate "each person as to whom there is reasonable ground to believe that such person will engage in, or probably will conspire with others to engage in, acts of espionage or sabotage." Obviously, speed will be of the essence and any diligent Attorney General charged with enforcing this Act must have a list of suspects prepared in advance. Data supposed to support such a list is doubtless lodged in the files of the FBI.

The FBI has long operated under a Department of Justice order providing:

> Except upon specific authorization of the Attorney General, no officer or employee shall forward to any person outside the Department of Justice . . . any information obtained from the Federal Bureau of Investigation . . . .[63]

But there are vaguely authorized exceptions. Department regulations

---

61 From a careful study of all available data, Professor Ralph Brown concluded in 1958 that the federal program then covered more than 13 million people, or one-fifth of the national labor force. R. BROWN, LOYALTY AND SECURITY 181 (1958). The same fraction today would produce a figure in excess of 16 million. U.S. BUREAU OF THE CENSUS, STATISTICAL ABSTRACT OF THE UNITED STATES 213 (1970). Professor Brown also estimated that the cumulative total of those dismissed under the program in 1958 was in excess of 10,000. R. BROWN, *supra*, at 182. It is a fair guess that their names, and the names of many others who were not dismissed but about whom derogatory information was recorded, are included in the FBI files. But there is no reason to suppose that all of them are included in the 1.7 million files reported in the National Crime Information Center.

62 50 U.S.C. §§ 811-826 (1964).

63 Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2, 11 n.10 (1956). *See also* United States *ex rel.* Touhy v. Ragen, 340 U.S. 462 (1951). This order is still in effect. Letter from Helen W. Gandy, Office of the Director, FBI, March 23, 1971.

allow for exchange of "identification records, including personal fingerprints voluntarily submitted," with "law enforcement and other governmental agencies" and the operation of "a central clearinghouse of police statistics . . . and a computerized nation-wide index of law enforcement information under the National Crime Information Center."[64] And "the FBI has long followed a policy, approved by several Attorneys General, of relaying information believed to be of interest to other Government agencies."[65] Moreover, although the official position of the FBI forbids disclosure of files to private parties, there is reason to doubt adherence in the field.[66]

2. The Internal Revenue Service.—Most adults in the country are required to initiate a file with the IRS by filing a tax return. The file is augmented when the IRS launches an investigation of tax liability or has to resort to collection efforts.

In 1965 the Commissioner of Internal Revenue admitted[67] to a Congressional committee that the Service had in the past used two-way mirrors and bugging devices in conference rooms where taxpayers and their lawyers met prior to and during discussions with IRS agents. The Commissioner further admitted that some agents, in an excess of "zeal emanating from the highest motives," had employed illegal bugs and wiretaps. He assured the committee that all such practices had been terminated.[68] Another practice, not disavowed by the IRS but now forbidden by Congress, involved the opening of a taxpayer's first class mail, either in search of evidence of tax liability or in search for assets from which taxes might be collected.[69]

---

64 28 C.F.R. § 0.85 (1970); *cf.* 28 U.S.C. § 534 (1964).

65 Hoover, *A Comment on the Article "Loyalty Among Government Employees,"* 58 YALE L.J. 401, 403 (1949).

66 Mayor Alioto of San Francisco recently told a Senate subcommittee that he had proof that the FBI had supplied information to *Look* magazine for an article charging him with underworld connections. N.Y. Times, March 4, 1971, at 22, col. 1. [This and all subsequent citations to newspaper reports of testimony refer to testimony in hearings currently being conducted by the Subcommittee on Constitutional Rights of the Senate Judiciary Committee.] The Department of Justice replied that an FBI agent had not "furnished," but had "confirmed," information which the magazine might have obtained from other federal agencies and that the agent involved had been disciplined and forced to retire. N.Y. Times, March 10, 1971, at 1, col. 6; Washington Post, March 10, 1971, at 1, col. 4.

67 *Hearings on Invasion of Privacy (Gov't Agencies) Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 89th Cong., 1st Sess., pt. 3, at 1130, 1133-1143 (1965).

68 Later the Commissioner advised the Committee that the agents engaging in illegal eavesdropping had been disciplined by reprimand and transferred and that there had been some voluntary separations from the service. *Hearings on S. 928 Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 90th Cong., 1st Sess., pt. 2, at 116 (1967). There was, of course, no mention of criminal prosecution.

69 Federal statutes forbid, and prescribe criminal penalties for, the opening of first class letters or parcels by anyone save an employee in the dead letter office or a person holding a search warrant. 18 U.S.C. § 1072 (1964); 39 U.S.C. § 4057 (1964). *See also* 39 C.F.R. § 117.1 (1970). But it is a nuisance to obtain a search warrant, the application for the warrant must make some showing of probable cause for the search, the warrant may be

It might be supposed that information that the government compels the citizen to supply in his tax returns would be held in confidence and used only for the purpose for which it is supplied. In fact, the confidentiality of tax returns is preserved by a statute that has all of the containing qualities of a sieve.[70] Tax returns are fully available to state tax officials,[71] to any Congressional committee "authorized to investigate returns," and to anyone authorized by Executive Order.[72]

3. The Armed Services.—The Army, of course, has personal files on those who are, or have been, in its service. In addition, as a former captain of Army intelligence recently revealed, the Army since 1965 has been collecting information on civilians in its computerized data bank at Fort Holabird in Baltimore, ostensibly to enable the Army to anticipate civil disturbances.[73] Subsequently, the Army assured a congressman that the surveillance of civilians would cease and that all

---

annoyingly specific about the items to be seized, and there have even been instances where warrants have been refused. Hence, the IRS hit upon a more "efficient" scheme.

Provisions of the Internal Revenue Code authorize the IRS to make its own administrative levy on "property of" a taxpayer "for the payment of" taxes. 26 U.S.C. § 6331 (1964), *as amended*, (Supp. V, 1970). These provisions also direct that "as soon as practicable after the seizure of the property" it shall be sold. 26 U.S.C. § 6335 (1964), *as amended*, (Supp. V, 1970). In any event, they reach only to property of the taxpayer, and postal regulations provide that the sender of mail may reclaim it at any time before it is delivered to the addressee. 39 C.F.R. § 153.5 (1970). Nonetheless, it was the practice of the IRS to serve levies on the Post Office and the practice of the Post Office to surrender undelivered mail addressed to taxpayers—not for the purpose of sale, but for the purpose of opening and examining by the IRS. *Hearings on Invasion of Privacy (Gov't Agencies) Before the Subcomm. on Ad. Practice & Procedure of the Senate Judiciary Comm.*, 89th Cong., 1st Sess., pt. 2, at 352-54, 360-61, 366-67, 369-71, 380-86 (1965). When this practice was exposed, Congress promptly amended the Internal Revenue Code to exempt all undelivered mail from the IRS levy. 26 U.S.C. § 6334(a)(5) (Supp. V, 1970).

[70] 26 U.S.C. § 6103 (1964), *as amended*, (Supp. V, 1970).

[71] It has been reported that at least 45 million of some 75 million returns filed in 1970 were put on computer tapes and mailed to at least 30 states. Wall St. J., April 21, 1970, at 1, col. 6.

[72] Between 1957 and 1970 53 such orders have been issued. Historical note to 26 U.S.C.A. § 6103 (1967 & Supp. 1971). These orders are not confined to the returns of named persons, but authorize inspections of all returns for designated periods of years. They have opened the federal tax returns to various federal agencies and Congressional committees not charged with tax responsibilities. Two of the chief beneficiaries of these Presidential dispensations have been two committees that have nothing to do with internal revenue matters. One is the House Internal Security Committee (neé House Un-American Activities Committee). *See, e.g.*, Exec. Order No. 11465, 3 C.F.R. § 116 (1969). The other is the Senate Subcommittee on Internal Security. *See, e.g.*, Exec. Order No. 11505, 35 Fed. Reg. 939 (1970).

Moreover, in relying on these Executive Orders, I am substantially understating the extent to which tax returns or their contents are disseminated. Disclosures about a year ago that Presidential aide Clark Mollenhoff was examining tax returns without an Executive Order—or at least without a published order—led to further disclosures that similar practices were followed in the Kennedy administration. It was reported also that IRS employees had not infrequently leaked the contents of returns to others and that in one instance a friendly revenue agent had obliged a federal prosecutor by screening the tax returns of 150 prospective jurors in a tax case. No one could recall, however, that any IRS employee had ever been prosecuted under a statute, *e.g.*, 26 U.S.C. § 7213 (1964), imposing criminal penalties for such activities. Wall St. J., April 21, 1970, at 1, col. 6; Wall St. J., April 27, 1970, at 8, col. 2.

[73] Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASH. MONTHLY, Jan. 1970, at 4; N.Y. Times, Jan. 16, 1970, at 26, col. 1.

dossiers would be destroyed.[74] Belying this assurance was a later announcement by Secretary Laird that surveillance operations had been transferred to civilian control in the Department of Defense.[75]

In hearings currently in process before a Senate subcommittee, Defense Department spokesmen revealed[76] that since 1968 the Department has maintained an index of 25 million names that includes both civilians who have taken part in civil rights or antiwar activities, and prominent persons[77] friendly with such suspects. In defense of this practice, the Army assured Congress that its share of the dossiers—about 8 million—was accessible to only 688 authorized officials.[78] In addition, Assistant Attorney General William Rehnquist conceded abuses due to "excessive zeal," and testified that the surveillance of civilians has now been transferred from Defense to Justice. However, he opposed any legislative limitations on such surveillance and urged the Congress to rely upon the "self-discipline" of the executive branch.[79]

4. The House Internal Security Committee.—Not all the dossier compilers in the federal government are in the executive branch. Since 1938 the House Un-American Activities Committee (rechristened the House Internal Security Committee in 1969) has been compiling dossiers on persons and organizations not sufficiently anti-Communist to suit its tastes. (In a much more sporadic fashion, the Senate Internal Security Subcommittee has done the same thing.) Although the Supreme Court has ruled[80] that the Committee's procedures do not include minimum safeguards to insure the rationality of its compilations, these compilations are, nonetheless, widely used and easily available. Anyone can obtain a copy of a Committee dossier merely by having it requested by a member of Congress.[81]

---

74 N.Y. Times, March 13, 1970, at 26, col. 6.

75 N.Y. Times, Dec. 24, 1970, at 1, col. 2.

76 *See* remarks of Senator Birch Bayh, 117 CONG. REC. S. 2290 (daily ed. March 2, 1971); N.Y. Times, Feb. 26, 1971, at 8, col. 3; Boston Globe, Feb. 28, 1971, at 31, col. 1.

77 The list includes Senator Adlai Stevenson III, Representative Abner Mikva, and former Illinois Governor Otto Kerner. N.Y. Times, Feb. 13, 1971, at 31, col. 1.

78 Washington Post, March 3, 1971, at 1, col. 2.

79 N.Y. Times, March 10, 1971, at 1, col. 6; Washington Post, March 10, 1971, at 1, col. 4. Before the Congressional hearings started, the ACLU had filed two actions to enjoin the Army's civilian surveillance programs as a violation of the first and fourth amendments and of a constitutionally protected right of privacy. In each instance the complaint was dismissed, and in both cases appeals were taken. In one of the cases the Court of Appeals for the District of Columbia reversed and ordered the Army to trial. Tatum v. Laird, No. 24203 (D.C. Cir., Apr. 27, 1971); ACLU v. Westmoreland, 39 U.S.L.W. 2401 (N.D. Ill., Jan 5, 1971).

80 Dombrowski v. Pfister, 380 U.S. 479, 496 (1965).

81 During the past year the Committee responded to over 1000 such requests, and its files were also examined by 25 executive departments and agencies of the federal government. H.R. REP. No. 92-14, 91st Cong., 2d Sess., 166 (1970). In 1968 Congressman Don Edwards wrote to several executive agencies and departments and asked them to what extent they searched Committee files and why. All responded that they searched the files

The Committee publishes a cumulative index that includes the names of all individuals, organizations and publications mentioned in any of the various publications of the Committee. An index for the period 1938-54 included some 38,000 names of individuals;[82] a supplement published last year lists about 25,000 names mentioned between 1955 and 1968 in Committee reports, hearings or "consultations."[83] Of course one has no grounds to protest inclusion in a list which includes, among others, all known and suspected members of the Communist party and the Ku Klux Klan, since the Committee declares (in fine print) in the front of the index:

> The fact that a name appears in this index simply indicates that said individual, publication or organization has been mentioned in a hearing, report, or consultation. It is not per se an indication of a record of subversive activities. A careful check of references in the hearing, report, or consultation will determine the circumstances under which such individual, publication or organization is named.[84]

Anyone who has the time and access to the Committee's many hearings and reports can check out the basis for including most of the names in the listing. The Committee does not explain, however, how one is

in connection with the federal loyalty-security program and estimated the frequency of their searches as follows: Housing and Urban Development Dep't, "[A]bout once a month"; Health, Education and Welfare Dep't, "[S]everal times each week"; Defense Dep't, "[A]pproximately 120 times a week"; Civil Service Comm'n, "[A]pproximately 288,000 times in fiscal 1967." 114 CONG. REC. 6271-6272 (1968).

Congressman Edward Koch has recently introduced a bill, applicable only to the House Internal Security Committee, which would require the Committee to notify each individual on which it keeps a file, to allow the individual to inspect and supplement the file (but not learn the source of information in it), and to forbid any disclosure of the file outside the Committee and its staff without the consent of the subject—but with a blanket exception from all these provisions for files that two-thirds of the Committee decide should "be kept secret in the interest of national security." H.R. 841, 92d Cong., 1st Sess. (1971).

Last summer the Committee sent a questionnaire to 179 colleges and universities asking them to list all campus speakers for the previous two year period, together with the honoraria paid. By matching the replies received with its dossiers on those named, the Committee produced and released to the press a list of 65 "radical" campus speakers. N.Y. Times, Oct. 15, 1970, at 23, col. 3. Some of these listed protested and the list was pared down to 57.

The American Civil Liberties Union brought an action to enjoin official publication and distribution of the list. Judge Gesell decided that he could not direct an injunction to Committee members because of the speech or debate clause, U.S. CONST. art. I, § 6, cl. 1, but the court did enjoin the Public Printer from printing or distributing the list, which he found to have no legitimate legislative purpose, but to be designed solely to appeal to college officials, alumni and parents in an effort to inhibit free speech on the campuses. Hentoff v. Ichord, 318 F. Supp. 1175 (D.D.C. 1970). Although the government has appealed the decision, the Committee persuaded the House to adopt a resolution directing the Printer to publish the list and he has done so. *See* 116 CONG. REC. H. 11606-25 (daily ed. Dec. 14, 1970); H.R. REP. No. 91-1732, 91st Cong., 2d Sess. 7 (1970).

[82] CUMULATIVE INDEX TO PUBLICATIONS OF THE COMM. ON UN-AMERICAN ACTIVITIES 1938-54, at 15-961 (1962).

[83] SUPPLEMENT TO CUMULATIVE INDEX TO PUBLICATIONS OF THE COMM. ON UN-AMERICAN ACTIVITIES 1955-68, at 19-587 (1970).

[84] *Id.* at 1.

to check out its "consultations." Presumably one asks his Congressman to obtain a copy of the Committee's dossier on the subject.

5. The Census Bureau.—Although the Constitution directs a decennial "enumeration" of the population for the purposes of apportioning representatives among the states,[85] the Department of Commerce through the Census Bureau is now directed by statute to collect and publish information not only on the population but also on industry, business, agriculture, governments, on crime and on defective dependent and delinquent classes.[86] The population census, far from being a mere "enumeration," now covers matters of sex, race, national origin, place of birth, marital status, family size, nature of household, quality of housing, geographical location, and mobility.[87] In addition to information collected for itself, the Census Bureau also obtains information from other agencies, such as the Internal Revenue Service and the Social Security Administration.[88] Like the benevolent private compilers, the Census Bureau is interested not in individuals but in groups. But, as with private compilers, the Bureau's compilation cannot be kept up to date or programmed for new uses unless a key to the identity of each individual is preserved.

The law requires everyone over the age of eighteen to respond to the Bureau's inquiries.[89] The Bureau is authorized to furnish state governments, courts, and individuals with "data for genealogical and other proper purposes" although the information so furnished is not to be "used to the detriment of" the subject.[90] The Bureau is forbidden to use the information for "other than . . . statistical purposes" or to permit anyone outside the Department of Commerce to "examine . . . individual reports"[91] and criminal penalties are prescribed for unauthorized disclosure of information.[92]

---

85 U.S. CONST., art. I, § 2, cl. 3.

86 13 U.S.C. §§ 101-61 (1964).

87 Not all 200 million of us answer all questions. In the 1970 census, 80% received short form questionnaire covering age, race, marital status and housing. Fifteen percent received a longer form and 5% received the longest form. N.Y. Times, April 1, 1970, at 4 col. 4. A citizen's attempt to compel the Bureau to frame inquiries that would lay the basis for reduction in the Congressional representation pursuant to § 2 of the fourteenth amendment for states discriminating against voters on the basis of race ended in dismissal of his complaint in Lampkin v. Connor, 360 F.2d 505 (D.C. Cir. 1966). *See also* Prieto v. Stans, 321 F. Supp. 420 (N.D. Cal. 1970).

88 *Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 28 (1966).

89 13 U.S.C. § 221 (1964). *See* United States v. Sharrow, 309 F.2d 77 (2d Cir. 1962), *cert. denied*, 372 U.S. 949 (1963). The fourth amendment offers no protection. United States v. Rickenbacker, 309 F.2d 462 (2d Cir. 1962), *cert. denied*, 371 U.S. 962 (1963).

90 13 U.S.C. § 8 (1964).

91 13 U.S.C. § 9(a) (1964).

92 13 U.S.C. § 214 (1964).

The Bureau claims that there has never been a known violation of these restrictions on use and that it does not supply individual information to other federal agencies.[93] But the Federal Trade Commission found a loophole. Pursuant to an investigation of possible violation of antitrust laws, it issued an administrative subpoena for a corporation's file copy of its census returns. The Supreme Court, in an opinion equally applicable to all census returns and probably to tax returns as well, held that the subpoena should be judicially enforced although the "confidential" census report form stated that it could not "be used for purposes of taxation, investigation or regulation." Both the legend on the forms and the statutory restrictions on disclosure were held to run only against the Census Bureau and not to impose limitations on the power of other governmental agencies to compel the subject to disclose its file copies.[94] Congress promptly amended the law to forbid any governmental agency to obtain copies of census returns retained by the subject.[95]

This survey of official dossier compilers is by no means complete, even at the federal level. For instance, an Associated Press study last year reported that the Civil Service Commission has files on 10 million persons who have sought federal jobs since 1939 and additional files on 1.5 million suspected of "subversive activities," all of whom presumably have lost or will never obtain federal employment. The Secret Service also has computerized 100,000 names and accumulated 50,000 dossiers.[96] Personal files are also kept on virtually all of the labor force by the Social Security Administration and the Passport Office keeps a computerized file of more than 243,000 citizens whose applications for passports are to be brought to the attention of law enforcement agencies.[97] A 1966 survey of all federal executive departments and agencies revealed that they had 3.1 billion personal files, including 264.6 million police records, 342 million medical histories, 279.6 million psychiatric records and 187.8 million "security or other investigative reports."[98]

Congressman Edward Koch and Senator Birch Bayh have intro-

---

93 *Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 27-28 (1966).

94 St. Regis Paper Co. v. United States, 368 U.S. 208 (1961).

95 13 U.S.C. § 9 (1964).

96 Boston Herald-Traveler, April 19, 1970, at 43, col. 1.

97 N.Y. Times, Feb. 11, 1971, at 11, col. 1.

98 SENATE SUBCOMM. ON AD. PRACTICE & PROCEDURE, GOV'T DOSSIER (SURVEY OF INFORMATION CONTAINED IN GOV'T FILES) 90th Cong., 1st Sess., 19, 26-27 (Comm. Print 1967). *See also The Computerization of Government Files: What Impact on the Individual?*, 15 U.C.L.A.L. REV. 1371 (1968); S. WHEELER, ON RECORD (1969).

duced bills[99] to enact a Citizen's Privacy Act. Applicable to all federa agencies and departments subject to the Administrative Procedur Act—but not to Congressional committees—the Act would impose th same requirements of notice to the subject and opportunity to supple ment the file and nondisclosure without the subject's consent a Representative Koch's bill would impose on the House Internal Secu rity Committee[100]—but with exceptions for files "compiled for la enforcement purposes" so long as "reasonably necessary to commenc prosecution or other action" and for files "specifically required b Executive order to be kept secret in the interest of the national secu rity."

III. Toward a National Data Bank: Dangers and Inadequate Safeguards

As previously indicated, there was a proposal a few years ag originating with certain academics and encouraged by the Bureau c the Budget, to establish a Federal Data Center, not for the purpose c compiling personal dossiers, but solely to compile statistical inform tion on groups. During Congressional hearings it was conceded that som

---

99 H.R. 854 & S. 975, 92d Cong., 1st Sess. (1971).

100 *See* note 81 *supra*.

What the federal government is doing in this area, the states are doing also. The Ne York State Identification and Intelligence System, established in 1965, has a computeriz central data bank serving 3,600 law enforcement agencies in the state. N.Y. Times, Mar 11, 1971, at 26, col. 4. The Oklahoma Office of Inter-Agency Coordination, established 1969 with Federal Law Enforcement Assistance funds, is now facing an ACLU lawsu seeking the dismantling of 6,000 dossiers. Civil Liberties, February, 1971, at 1, col. Civil Liberties, October, 1970, at 1, col. 1. The Massachusetts Civil Liberties Union preparing a similar suit against the State Police's Subversive Activities Division, who continued operation is also being challenged in the state legislature. The Docket, Februa 1971, at 1, col. 3. In a New Orleans suit now before the Fifth Circuit the commander the city's intelligence division has testified that his men attend and take photograp at all public events at which "controversial" views are likely to be expressed. Ci Liberties, July, 1970, at 2, col. 1. In New Jersey, the Attorney General sent a memorandu to all local law enforcement officials asking them to report to the State Police Centr Security Unit the names of all persons involved in "incidents" such as "civil disturban riot, rally, protest, demonstration, march, confrontation, etc.," including information spouses, draft status, affiliations, education and credit status. In a class action for a declar tory judgment that such a program violated the first amendment, the trial court ga summary judgment for the plaintiffs and ordered the Attorney General to produce a destroy all dossiers except when they "will be used to charge persons with specifica defined criminal conduct." Anderson v. Sills, 106 N.J. Super. 545, 256 A.2d 298 (Ch. 196 On appeal, the decision was reversed and remanded. The summary judgment was he improper because the supreme court seemed to view as fanciful plaintiff's fears that t dossiers would be improperly used. Anderson v. Sills, 56 N.J. 210, 265 A.2d 678 (1970) (amended complaint has been filed in the case). For discussion of the trial court decisio see Askin, *Police Dossiers and Emerging Principles of First Amendment Adjudication*, Stan. L. Rev. 196 (1970). *See also* Comment, *Secret Files: Legitimate Police Activity Unconstitutional Restraint on Dissent?*, 58 Geo. L.J. 569 (1970); Note, *Chilling Politic Expression by Use of Police Intelligence Files*, 5 Harv. Civ. Rights-Civ. Lib. L. Rev. (1970).

key to the identity of those in the group must be maintained if the group compilations were to be kept current and remain adaptable to new uses.[101] In consequence a commitment was obtained from the Bureau of the Budget that before such a central data bank would be established, the problems of threat to privacy would be first evaluated by a panel of constitutional lawyers, computer experts, suppliers and users of statistical information, and representatives of Congress.[102] Although no further action has been taken, one should not conclude that the issue of a National Data Bank is an issue for another day. The vast numbers of personal dossiers already assembled by private and official compilers have effectively created a "National Data Bank" now. While a truly centralized National Data Bank might be more efficient, the present system is more vulnerable to unauthorized use and abuse.

Computerization by both private and governmental compilers is rapidly facilitating the advent of a national, centralized system. Many noncomputerized compilers are either in the process of computerizing or are feeding their dossiers into the computers of other compilers. The federal government, which acquired its first all-electronic computer during World War II, was using over 2000 computers by 1964.[103]

The computer can store infinite bits of information and can retrieve them within a few billionths of a second.[104] Computers can be connected by interfaces and can be tapped, not only by theft of printouts or by wires, but also by laser beams and other non-mechanical intrusions. Access codes can be and are broken, after which the intruder can "display and manipulate the data stored within the system."[105] No completely effective security system against such intrusions has been or probably ever will be devised.[106]

The intruder seeking data about a particular individual needs to locate a key to the pertinent data, but this task in many cases may not pose much difficulty. Enough advance knowledge about the subject to pose a few pertinent questions to the raided computer will quickly

---

101 *See* hearings cited in note 35 *supra*.

102 H.R. REP. No. 1842, 90th Cong., 2d Sess. 22-23 (1968).

103 H.R. REP. No. 802, 89th Cong., 1st Sess. 6 (1965); HOUSE COMM. ON POST OFFICE AND CIVIL SERVICE, 1964 INVENTORY OF AUTOMATIC DATA PROCESSING (ADP) EQUIPMENT IN THE FEDERAL GOVERNMENT, 88th Cong., 2d Sess. 3, 10c (1964).

104 Miller, *Personal Privacy in the Computer Age*, 67 MICH. L. REV. 1091, 1095 (1969). Since these remarks were written Professor Arthur Miller has also published his valuable book, THE ASSAULT ON PRIVACY (1971).

105 Miller, *supra* note 104, at 1111, 1190; A. WESTIN, PRIVACY AND FREEDOM 79-80 (1967).

106 Testimony of Robert P. Henderson, Vice-President, Honeywell Information Systems, before Subcomm. on Constitutional Rights of Senate Judiciary Comm., 92d Cong., 1st Sess. (1971).

identify the subject. In other cases, an even easier key may be available: social security numbers.[107]

Computers not engaged in compiling dossiers or in tapping those that are can also make their contributions to the data bank. The airlines' computerized reservation service will reveal where you flew, whether you reserved a rental automobile for use there, and, perhaps, where you made hotel reservations. The hotels' computerized reservation service will reveal the latter information if the airlines' service does not, and will reveal also whether you shared the accomodation with one claimed to be your spouse. Your bank's computerized check processing system will reveal details of many of your expenditures and, as we move on to the checkless, cashless society, will ultimately reveal the details of your every expenditure.

Against this monstrous technological capacity to search out most of the details of our lives, the present state of the law and of most proposals for new law seem both inadequate to achieve their professed objectives and inadequate in the protection afforded even if those objectives could be achieved.

A. Insuring the Accuracy of Dossiers

Concern about the accuracy of the dossiers reflects what the computermen identify as the GIGO principle—Garbage In, Garbage Out. In fact, the computerization of personal dossiers may reflect the first literal application of that principle. Those investigating the personal characteristics of individuals have been known to comb through the subjects' garbage for clues.

The main thrust of the Fair Credit Reporting Act,[108] and of the proposals for legislative restrictions on some federal compilers,[109] is to attempt to insure that the information in our dossiers will be accurate. The chief mechanism to achieve this end contemplates notice to the subject with an opportunity for him to correct erroneous entries. These measures almost surely will not achieve their objectives for at least two reasons:

1. Failure to Receive Notice.—Many subjects will never receive notice of their dossiers. The only sanctions in the Fair Credit Re-

---

107 Social security numbers are entered on federal and many state tax returns. In many states the number is also one's drivers license number. One and a half billion of those 3.1 billion federal personal files also contain the subject's social security number. SENATE SUBCOMM. ON AD. PRACTICE & PROCEDURE, GOV'T DOSSIER (SURVEY OF INFORMATION CONTAINED IN GOV'T FILES), 90th Cong., 1st Sess. 26 (Comm. Print 1967).

108 84 Stat. 1114, tit. VI (1970 U.S. CODE CONG. & AD. NEWS 5142); *see* note 30 *supra*.

109 *See* note 81 & text accompanying notes 99, 100 *supra*.

porting Act are compensatory damages for negligent failure to give notice and punitive damages for wilful failure to give notice. Since the subjects who do not receive a notice will never know that they have a cause of action, there is a considerable incentive for compilers to be sparing with the notices.

The incentive to give notice is even less for compilers who are not excepted in "law enforcement" and "national security" cases under the proposed legislation applicable to executive departments and agencies, since the proposed law contains no sanctions of its own. It seems highly doubtful that the nebulous provisions of the Federal Tort Claims Act can be read to incorporate the compensatory damage provisions of the Fair Credit Reporting Act for failure to give notice.[110] Beyond this, there appears to be only the possibility of a mandamus action to compel compliance;[111] but this possibility is of little value to one who is unaware that he is the subject of a dossier. The proposed legislation applicable to the House Internal Security Committee also contains no sanctions of its own and seems even more toothless. The Federal Tort Claims Act extends only to executive departments and agencies;[112] a mandamus action may not reach members of Congress[113] and apparently will not reach Committee employees if the Committee is careful not to delegate to them the duty of giving notice.[114]

2. Inadequacy of the Remedy.—The credit reporting agencies succeeded in selling Congress the monstrous proposition that they should remain free to collect and disseminate erroneous dossiers—subject only to liability for malice or wilful intent to injure—and that the burden should fall upon their subjects to come forward and correct errors. The pending bills applicable to some federal compilers proceed on a similar assumption. But many subjects, even if they do receive notice, may conclude that life is too short, or their resources too limited, to make an effort toward correction. Particularly may they

---

110 Liability is imposed on the United States for compensatory but not punitive damages for negligent or wrongful acts or omissions of officers and employees of executive departments and agencies "under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred" [28 U.S.C. § 1346(b) (1964)], and for damages "in the same manner and to the same extent as a private individual under like circumstances," 28 U.S.C. § 2674 (1964). In any event the liability does not extend to "an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation . . ." 28 U.S.C. § 2680 (1964).

111 28 U.S.C. § 1361 (1964) gives the federal district courts original jurisdiction "of any action in the nature of mandamus to compel an officer or employee of the United States or any agency thereof to perform a duty owed to the plaintiff."

112 28 U.S.C. § 2671 (1964).

113 *See* Hentoff v. Ichord, 318 F. Supp. 1175 (D.D.C. 1970).

114 *See* note 110 *supra*.

reach this conclusion when they discover that they can neither learn the sources of adverse entries (except for credit bureau reports), nor compel deletion of such entries, but must content themselves with entering their version of matters in the file.

B. Restricting Access to Dossiers

The Fair Credit Reporting Act imposes two types of restrictions on access to the dossiers of commercial compilers without the consent of the subject. First, the compiler may furnish information only to persons and governmental agencies whom the compiler "has reason to believe" have a "legitimate business need" for the information. Any compiler that is negligent in determining its "reason to believe" is liable for compensatory damages, and any compiler that wilfully acts without such "reason to believe" may be liable for punitive damages. These remedies will doubtless be invoked almost as rarely as the criminal penalties prescribed for any compiler who knowingly and wilfully discloses information to an unauthorized individual. The standard for authorized access—"legitimate business need"—is very possibly too vague to satisfy due process requirements for a criminal statute and is certainly too vague to hold out much promise for an effective civil remedy.

Second, the Fair Credit Reporting Act forbids disclosure of more than identifying information concerning name, address and employment to any government agency that does not have a "legitimate business need"—except in response to court order. The restriction imposes no substantive limit upon governmental agencies empowered to issue subpoenas enforceable by court order though it does impose the procedural inconvenience of obtaining a court order.[115] This does not include the FBI, which has no subpoena power. Instead the FBI is left with three alternatives: first, it can stop using the files of the commercial compilers; second, its agents can obtain access to the files by means of false pretenses and risk prosecution by the Department of Justice; or third, its agents can without false pretenses persuade the commercial compilers to risk prosecution by the Department of Justice by knowingly and wilfully making an unauthorized disclosure. The record of Department of Justice prosecutions for illegal wiretaps under the Communications Act of 1934 strongly suggests that the FBI will not feel confined to the first alternative.

The Fair Credit Reporting Act also authorizes disclosure of dos-

115 *See* note 22 *supra*.

siers pursuant to "the written instructions of" the subject. But obviously, when the subject is seeking employment, insurance or even credit this consent in many cases will be far from voluntary.[116] Similarly, the proposed legislation applicable to some federal compilers would—with generous exceptions for "national security" and "law enforcement" files—forbid disclosure of information without the "permission" of the subject. Here again, any consent given by a subject seeking federal employment will often not be voluntary. In any instance, the limited sanctions available under these proposals are likely neither to deter improper disclosure, nor to provide effective relief to one injured by disclosure.

C. Limiting the Contents of Dossiers

There have been suggestions that limitations be placed upon the content of personal dossiers. Some proponents of a formal National Data Center, for instance, suggested that its files include only "statistical" data and not the personalized data found in FBI, IRS, military, civil service and medical records.[117] But these proponents came up with no standard precise enough to permit effective control. Moreover, they apparently contemplated the continued compilation of dossiers that would not be included in the National Data Center, and it is the existence of these dossiers combined with the ubiquitous computer that provides the present, informal, National Data Center. One proposed version of the Fair Credit Reporting Act sought to forbid commercial compilers from reporting "information which is not reasonably relevant for the purpose for which it is sought or which constitutes an undue infringement of the individual's right of privacy."[118] The compilers were able to persuade Congressmen that this restriction was intolerably vague.

With the present state of knowledge about the contents and the uses of dossiers, it seems unlikely that we can effectively define either the "legitimacy" of the "need" permitting access, or what information is "relevant" to that need. Even less can we define the balance to be struck between the "need" and a desirable preservation of privacy.

---

116 Indeed, one of the compilers' arguments against compelling them to give the subject a copy of his dossier was that someone else might, by economic coercion, "invade his privacy" by compelling him to produce it. *Senate Credit Bureau Hearings I, supra* note 1, at 65; *Senate Credit Bureau Hearings II, supra* note 1, at 226.

117 *See* Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 413-414 (1968).

118 H.R. 16340, 91st Cong., 2d Sess. § 54 (1970).

IV. But What About Privacy?

Even if all dossiers were absolutely accurate, or if remedies for inaccuracy were completely adequate, the question of the right to privacy would remain. By a "right to privacy" I do not mean to confine myself to the right to protection against unwanted publicity and palpable intrusion into private affairs that finds limited protection in some jurisdictions.[119] Nor do I confine myself to those recently emerging constitutional concepts that thus far have forged only slightly beyond the fourth amendment to permit married persons to receive birth control information,[120] or to allow individuals to contemplate obscene material in the sanctity of their own homes.[121]

I refer instead to a concept of privacy confined neither to protection against publicity nor to palpable intrusions, to a concept that Justice Brandeis described as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[122] Justice Douglas has characterized this concept as the freedom of the individual "to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing."[123] As others have said, "the essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others."[124] Such a concept of privacy is offended by the gross compilation of personal details, however accurately and delicately the dossier be compiled, and by the dissemination of those details whether to private or public users of the information and regardless of their number.

It seems inconceivable that courts or state legislatures, either by developing legal remedies or expanding constitutional safeguards, will establish this concept of privacy in time to meet the dangers of the computerized dossier. Only the Congress seems capable of acting with the requisite speed. And, in order for it to act effectively, it must first come to comprehend the concept of privacy that its efforts must be de-

---

119 *See* text accompanying notes 25-28 *supra*.

120 Griswold v. Connecticut, 381 U.S. 479 (1965).

121 Stanley v. Georgia, 394 U.S. 479 (1965). This decision is already suffering some erosion. *See* United States v. Thirty-Seven Photographs, 39 U.S.L.W. 4518 (U.S. May 3, 1971); United States v. Reidel, 39 U.S.L.W. 4523 (U.S. May 3, 1971).

122 Olmstead v. United States, 277 U.S. 438, 478 (1928) (dissenting opinion).

123 Warden v. Hayden, 387 U.S. 294, 323 (1967) (dissenting opinion).

124 Ruebhausen & Brim, *Privacy and Behavioral Research*, 65 Colum. L. Rev. 1184, 1189 (1965).

signed to insure. It must also rid itself of three misconceptions which it shares with many outside the Congress:

1. The misconception that whatever technology can produce should be used, although technology produces not because of need, but because production is possible.
2. The misconception that anyone who can show that information is useful, or comforting, to him in the conduct of private or public affairs has shown a "legitimate need" for its use.
3. The misconception that whatever is efficient is desirable.

If a meaningful concept of privacy be adopted and these three misconceptions be discarded, Congress could then approach the problem on the assumption that so long as dossiers exist on the present scale they will be used in disregard of whatever restrictions may be imposed on their use. Law enforcement officials "in an excess of zeal" will disregard those restrictions and, in an excess of tolerance, will not invoke criminal sanctions against themselves or others who similarly disregard those restrictions. And with the use of dossiers in its present magnitude, any privately enforceable remedies will not suffice to check unauthorized use.

The only hope for substantial protection of privacy against the computerized dossiers, therefore, is that they not exist—at least that they not exist on the present scale. And if the "legitimate need" for the dossiers were appraised as an actual need for a vital public purpose, rather than as a convenience or a comfort for any acceptable purpose, the great bulk of existing dossiers could be eliminated and the growth of dossiers in the future drastically curtailed. Careful study of the contents of various compilations, and careful consideration of the justification therefor, would be required before lines could be drawn. But it seems apparent that a rigorous application of the test of actual need for a vital public purpose would drastically clear the files.

To cite but a few examples: No such need justifies the retention in FBI files of all information amassed by it on all persons investigated in connection with a particular crime after the case has been closed. Similarly, there is no need to retain in both FBI and Civil Service Commission files the collection of gossip, rumor and hearsay—or even of hard facts—on an applicant for federal employment after his application has been denied. The only possible need for preserving keys to personal identity in the Census Bureau's population statistics is to facilitate keeping statistics current and adapting them to new

uses during the ten-year period between censuses. But is that need so vital, and could it not perhaps be met instead by taking a population census at more frequent intervals?

There is no need at all for the highly untrustworthy files of the House Internal Security Committee. There is even room to doubt the need for those permanent dossiers that constitute the life-blood of the credit bureaus. As previously indicated, they are as likely to induce as to preclude unwise credit extension. Yet the business volume of the users of dossiers is so high that their losses are almost infinitesimal.[125] If credit bureau customers can do this well on the unreliable information they now receive, how much worse would they do if left to their own devices? It is often assumed that without credit bureau dossiers losses would greatly increase, with a concomitant increase in the cost of consumer credit and a throttling of the economy based on that credit. However, this mere assumption has not been explored sufficiently to justify perpetuation of credit bureau dossier compilation.

A rigorous inquiry into the actual need for existing compilations would doubtless produce even louder incantations from compilers about efficiency. It is more efficient to preserve dossiers for future possible use than to require a new investigation of the subject whenever information about him becomes necessary, or helpful, or comforting. Certainly it is more efficient. But it is also more efficient to provide an accessible file of every police investigation of anyone ever made, no matter how unwarranted, against the possibility that another investigation may be made in the future. It is also more efficient for the Selective Service to provide the FBI with fingerprints and other data on all persons it processes against the possibility that a small percentage of them may be future law violators. It would also be more efficient to extend the Alien Registration Act[126] to civilians. But we have not, in this country, permitted efficiency to be the determining factor when individual liberty is jeopardized. Instead, we have opted against efficiency and in favor of constitutional guarantees against unlawful searches and seizures and self-incrimination and for jury trials in

---

125 I have asked many bankers and finance company representatives about their loss ratios on consumer receivables and have yet to be given a figure higher than 0.5%. In other instances the consumer finance companies have claimed a loss ratio of 1.5%. *See* J. CHAPMAN & R. SHAY, THE CONSUMER FINANCE INDUSTRY 24 (1967). The bankers have claimed 2%. P. McCRACKEN, J. MAO & C. FRICKE, CONSUMER INSTALLMENT CREDIT AND PUBLIC POLICY 116 (1965). But the latest word I have seen, from a spokesman for the American Bankers Association, is that on consumer transactions "in commercial banks the loss ratio is less than half a percent; it is perhaps now getting close to a quarter of 1 percent." *Senate Credit Bureau Hearings II, supra* note 1, at 322.

126 8 U.S.C. §§ 1301-1306 (1964).

criminal cases. In view of the massive threat to individual privacy posed by the present and growing body of computerized dossiers, efficiency will hardly serve as a justification for their preservation.

These are the assumptions on which Congressional inquiry should proceed. Recognizing these assumptions, Congress would doubtless conclude that most of our present National Data Bank must be wiped out, and that preservation of and access to the surviving dossiers must be restricted to an actual need to further a vital public purpose. Finally, mindful of these assumptions, Congress would not vest the policing of restrictions in the hands of the most probable violators.

We have not yet had an inquiry based on such assumptions. The time for that inquiry is overdue. The computerized dossiers are multiplying by the day. And we are only thirteen years from 1984.

A DIFFERENT VIEW OF PRIVACY

ALBERT W. ALSCHULER*

Professor Countryman's Orgain Lecture[1] is an important addition to the growing literature of privacy. It presents a comprehensive picture of the threat that modern technology and organization pose to our sense of control over basic information about ourselves. Professor Countryman calls for action: We cannot leave the cause of privacy to the forces of laissez faire. I fully agree.

I believe, however, that Professor Countryman's lecture shares one defect with a number of lesser studies. It focuses too much of its energy on the mechanisms that now exist for compiling and distributing information, and not enough on the concept of privacy that it seeks to advance. In my view, Professor Countryman's study, like other recent writing in the field, does not put first things first. Before one can sensibly decide what to do about proliferating data banks, one must reach some judgment concerning the extent to which an individual should be able to control the use of information about himself. A precise, substantive concept of privacy should precede any procedural solution, and Professor Countryman's own concept of privacy is, in my view, too often implicit rather than carefully thought out and expressed.

The result, when it comes to solution, is a proposal that is essentially backward-looking. It seeks to recapture the era before the computerized personal dossier and the national data bank came into existence. Professor Countryman urges that except in cases of "actual need for a vital public purpose," data banks containing personal information should be abolished. Because the technological revolution that surrounds us has diminished our sense of privacy, Professor Countryman apparently sees technology, and organization itself, as our villains.

In my judgment, this proposal and others like it tend to go both too far and not far enough. By focusing on today's mechanisms of sharing information, they protect substantive privacy only haphazardly. At the same time, these proposals would impose gratuitous hardship on persons whose right to use and share information Professor Countryman does not challenge.

---

* Professor of Law, University of Texas; B.A., Harvard, 1962; LL.B., Harvard, 1965.

1 Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEXAS L. REV. 837 (1971).

Consider just one example. Under Professor Countryman's proposal, a department store contemplating an extension of credit apparently would not have access to the files of a consumer credit bureau. Professor Countryman would not, however, require the store to extend or deny credit in darkness or on the basis of an applicant's grooming and personal appearance. The store would apparently be free to seek information from the customer himself, from the references that he provided, and from other individuals and commercial institutions as well. As Professor Countryman puts it, the store would be "left to [its] own devices."

Under this regime, I suspect that most department stores would quickly adopt a "long form" credit application that would itself invade the customer's privacy. The form would require a substantial amount of time and energy for the customer to complete. Following this paperwork, the store would delay each application for a number of weeks while it contacted the customer's references and "verified" the information that he provided.

The customer would repeat this process with every credit application, for there would be no mechanism by which he could "waive" his right to privacy and permit the accumulation of personal data by a credit bureau. (If there were such a mechanism, it would be difficult to prevent an information gatherer from automatically requiring a "waiver" as a condition of extending credit. The present situation might therefore be rapidly duplicated.)

The central point is one that Professor Countryman recognizes: abolishing the consumer credit bureau would be inefficient—not only for the commercial institution but for the customer as well. Professor Countryman's proposal would tend to consume the consumer in paperwork and delay and discourage him from seeking services that he would otherwise obtain and value.

Professor Countryman argues that we must rid ourselves of "the misconception that whatever is efficient is desirable," and it is true that there are many situations in which free men must sacrifice efficiency to the cause of human dignity. But efficiency, though not the end of human existence, is a value nevertheless. I believe that we should receive something in return for our trade. If the invasion of privacy turns out to be the same in the end, it might as well be done efficiently.

I do not deny that there would be some gain to privacy under Professor Countryman's proposal. For one thing, there might be a

gain in the accuracy of the information used by department stores and other commercial institutions. I am not, however, entirely sure. A system which looked to the customer himself as the primary source of credit information would make it more difficult for a commercial institution to learn a third person's lies about him—at the same time that it made it easier for the customer to lie successfully about himself.

Thus there would not necessarily be a net gain in the accuracy of information under Professor Countryman's proposal, but there might be a gain of a different sort. A financial institution could demand as much information about a customer's past under this proposal as it demands today; but if the customer himself were the primary source of this information, the inaccuracies in the final report would probably tend to favor the consumer rather than harm him. Whether our system of jurisprudence formally recognizes the fact or not, harm to the consumer is likely to be more painful than harm to the financial institution. A shift in the direction of the inaccuracies might therefore be desirable.

In addition to the danger of inaccuracy, a centralized data bank poses a danger that information given for one purpose may be used for another—for example, that friendly statements to a lady from the Welcome Wagon may, without the customer's knowledge or consent, be considered in passing on a credit application a few weeks or a few years later. Professor Countryman does not, however, rest his opposition to data banks primarily on the danger of inaccuracy and on the difficulty of confining access to information to the people we wish to have it. Even if the accumulated information were accurate and even if the rules limiting access to this information could be fully enforced, Professor Countryman would see the data bank as a threat to privacy. It is with this last proposition that I disagree. In my view, Professor Countryman has confused the medium with the message.

Under Professor Countryman's proposal, it would apparently be necessary to establish an impartial agency to review each accumulation of information to determine whether it served an "actual need for a vital public purpose." This agency might have an administrative power to order the destruction of files that did not meet its standards; or more likely, the agency might propose suitably detailed legislation to Congress or the state legislatures. (I note, in passing, that Professor Countryman's solution seems inconsistent with his earlier statement,

"With the present state of knowledge of the contents and the uses of dossiers, it seems unlikely that we can effectively define either the 'legitimacy' of the 'need' permitting access, or what information is 'relevant' to that need. Even less can we define the balance to be struck between the 'need' and a desirable preservation of privacy." Professor Countryman would strike the balance somewhat differently from the people he criticizes, but he attempts essentially the same task. I think that Professor Countryman was right the second time around, and that the task should be attempted.)

My own approach to the problem of safeguarding privacy would, however, be somewhat different. In one respect, I would carry Professor Countryman's proposal farther. My initial inquiry would not be what information should be contained in a data bank (a particular *means* of storing and coordinating information), but what information an individual or institution should *have* in making a particular decision. In other words, I would ask the substantive question first.

As early as 1949, the Commonwealth of Massachusetts made it an "unfair educational practice" for an educational institution "to cause to be made any written or oral inquiry concerning the race . . . color or national origin of a person seeking admission . . . ."[2] I would take this legislation as my model and direct my hypothetical "privacy agency" (which I would borrow from Professor Countryman) to focus on each of the major tasks for which public and private groups now accumulate personal information—such tasks as deciding whether to extend or deny credit, deciding whether to hire or fire, investigating crime, census-taking, and so forth. In each instance, the agency should ask what sort of information ought to be available in performing the task; and as Professor Countryman notes, the inquiry should encompass not simply the relevancy of the information, but the extent to which this information is properly viewed as private.

The final proposals of the agency might be either negative or affirmative in form: "An employer shall not make or cause to be made any inquiry into the race of an applicant for employment, into arrests or criminal proceedings involving the applicant which were not followed by convictions, into an applicant's political associations or beliefs [with an exception, perhaps, for a few "national security" positions and for organizations like the Republican Party and the NAACP which have avowed political purposes] . . . ." Or, "A person or organi-

2 MASS. ANN. LAWS ch. 151C, § 2 (1958).

zation which employs more than five persons may make only the following inquiries concerning a person seeking employment as an unskilled laborer . . . ."

The resulting "privacy code" would be neither short nor simple, and it would undoubtedly be necessary to draw some difficult distinctions. I believe, however, that an agency that studied the current practices of various public and private investigators, the forms currently used to gather personal information, and the character of the specific problems that emerged could arrive at a consensus that would better reflect our concern for privacy than today's passive system of laissez faire.

Once the substantive question of how much personal information should be available in performing each task had been settled, it would be necessary to turn from the "message" to the "medium." The fact that a department store might be entitled to know a customer's weekly income before deciding whether to open a charge account for him would not mean that the store could learn this information by installing an electronic eavesdropping device in his place of business. Some techniques for gathering and sharing information should be, and some have been,[3] outlawed; and other techniques should surely be confined and regulated.

Whether the computerized data bank should be prohibited for most purposes seems to me to turn on the extent to which it augments the dangers of inaccuracy and of access for unintended purposes, and on the extent to which these dangers are offset by the affirmative uses of the data bank in sharing information. I am not nearly so pessimistic as Professor Countryman concerning the ability of governmental regulation to minimize the dangers.

Suppose, for example, that whenever a person or organization secured information from a consumer credit bureau, a statute required notice to the consumer of the identity of the information-user and of the information that he had obtained. Professor Countryman argues that this regulation might be evaded; a person who did not receive the required notice would usually be unaware that his rights had been violated. We could, however, test the credit bureaus' reporting practices through our own "dummy" requests for information; and even without this stratagem, it seems likely that any regular, systematic pattern of violation would eventually be discovered. Our sanctions could probably be made severe enough that the credit bureaus

[3] *See* 18 U.S.C. §§ 2510-2520 (Supp. V, 1970).

would be unwilling to run the risk. Moreover, if necessary, we could move beyond the private lawsuit as our sole enforcement mechanism. We could, for example, physically inspect and test the credit bureau's computers to ensure that they had been programmed to give the required notice. Indeed, we might be able to enlist computers to perform this task. My purpose, of course, is not to argue for a particular form of regulation, but simply to illustrate the existence of a range of regulatory techniques short of the large-scale file-burning that Professor Countryman proposes.

In setting forth a scheme for resolving privacy problems different from Professor Countryman's, I have made the point that I started out to make. We should employ a two-step analysis, asking first what information is "none of the information-user's business" and then what methods should be available to collect, store, use, and communicate information that the user is reasonably entitled to have in making a particular decision. This scheme does not carry us very far, of course, toward an ultimate solution, and it may be appropriate to add a few words concerning the character of the inevitable balancing process—whether that process is focused on the information that should be contained in a data bank as Professor Countryman proposes, or on the information that a person or group should have in making a particular decision as I suggest.

Unlike Mr. Justice Black, dissenting in *Griswold v. Connecticut*,[4] I do not value my privacy as much as the next man—at least when the next man is Professor Countryman. An individual's concern for privacy is itself a private and subjective thing. Professor Bruno Bettelheim has written, "[P]rivacy is not a universal, absolute good, but belongs very much to a particular style of life—to a historical period, a social class—and is thus culture bound."[5] Professor Bettelheim notes that what one generation could discuss only in the carefully guarded privacy of a darkened psychoanalytic treatment room, another generation sets forth in family magazines and on the screen. The ideal of one generation may be a separate bedroom and bathroom for each child, but when the child grows up, he may choose a commune where a dozen people sleep, love, and live together in a single room.

Because our concern for privacy is ad hoc, subjective, changing, and culture-bound, the extent to which an individual should be able to control the use of information about himself cannot be determined

[4] 381 U.S. 479, 510 (1965) (Black, J., dissenting).

[5] Bettelheim, Some Comments on Privacy 2 (unpublished manuscript on file at the University of Texas Law Library).

"in the large." No universal solvent can, in a few words, resolve all privacy problems. It is for this reason that I have suggested that a governmental agency approach the problem of safeguarding privacy "in the specific," by focusing on the most common uses of personal information and by evaluating the propriety of each use. In this way, we may be able to give effect to general cultural sentiments concerning privacy—sentiments that, in Justice Holmes' phrase, may lie tangled beneath the surface without losing their validity. Professor Countryman's test of "actual need for a vital public purpose" would, in my view, confuse our inquiry rather than aid it.

Professor Countryman writes, "The only hope for substantial protection of privacy against the computerized dossiers . . . is that they not exist—at least that they not exist on the present scale." Professor Countryman does not, however, describe what a "computerized dossier" is, and his statement could have far-reaching implications.

For example, Professor Countryman and I were both opposed to the confirmation of G. Harrold Carswell as a Justice of the Supreme Court. The battle over the Carswell nomination began, for all practical purposes, when a newspaper reporter discovered an interesting piece of personal information about Judge Carswell. A full generation before his nomination, Judge Carswell had said, "I yield to no man . . . in the firm, vigorous belief in the principles of white supremacy, and I shall always be so governed."

The reporter found this statement in a newspaper "morgue," which, of course, is an old-fashioned word for data bank. The newspaper files had not been placed on a computer tape, but I cannot believe that the newspaper's reliance on a manual filing system could make a critical difference. I, for one, am not distressed that the government had not combed through these files a dozen years earlier and discarded all material not shown to serve an actual need for a vital public purpose. Judge Carswell lost control over a bit of information about himself, but the right of privacy of a public figure with respect to his public statements should, I think, be very limited. Indeed, I believe that it would be unconstitutional to forbid a newspaper from maintaining a "morgue" unless the government agreed that it served an actual need for a vital public purpose.

A newspaper itself is a data bank, full of personal information, yet a newspaper surely could not be required to justify itself in terms of Professor Countryman's standard. My point is that file-burning is not very different from book-burning; the difference between a file

and a book is simply a printing press. There are, of course, instances in which the media should be restricted in the interest of preserving privacy, and there are instances in which file-compilers should be restricted as well. In both situations, our traditional concern for openness should argue for caution and restraint.

The history of the Carswell nomination illustrates one other point. The uses of information are contingent and unforeseeable. Today's idle curiosity may become tomorrow's actual need for a vital public purpose. Even the Massachusetts statute forbidding educational institutions from asking the race of applicants for admission has had an unforeseen impact. At the time that this statute was passed, the perceived danger was that schools and colleges would discriminate against the members of minority races. More recently, many schools have favored applicants from minority races—in the interest of securing greater balance among their student bodies, in the interest of advancing the status of members of these races in society at large, and in recognition of the possibility that traditional admission criteria may not adequately measure the abilities of many minority group students. This new educational policy has been hampered by the legislatively decreed absence of racial inquiry on college admission forms. Of course the policy of the Massachusetts statute can still be defended, and the current approach of the educational institutions can be criticized. Nevertheless, the legislative restriction has had an effect that was probably unintended. This restriction has impeded a program that the legislators themselves might have considered valuable, had they thought about it.

The standard of "actual need for a vital public purpose" seems to me, not only to underrate the virtues of information-sharing, but to oversimplify a difficult problem. I doubt that even actual need for a vital public purpose could justify some compilations of information—for example, any compilation achieved through non-governmental electronic surveillance. Yet even curiosity might justify a compilation of the published speeches of a public figure. It is necessary to focus, not only on the character of the need, but on the character of the information and the methods used to obtain it. Among the factors which we should consider are the relevancy of particular information to particular tasks, the extent of the need for this information, the extent to which the information is commonly viewed as private, the ability of particular techniques to supply the information accurately, the availability of substitute techniques, the extent of the intrusion

produced by each technique, the likelihood of use for unintended purposes, whether the individual has in any way consented to the intrusion or the information-sharing, and the character of the consent that he has given.[6]

A paper of this sort inevitably contains more criticism than praise. The extent of my agreement with Professor Countryman may therefore not be apparent. My goal is certainly not to minimize the dangers that Professor Countryman has set forth in graphic detail, nor to denigrate the need for prompt governmental action.

It has been suggested that the computer may expand man's ability to know and reason to greater extent than the automobile expanded his mobility; and this development, hopeful though it is, poses a serious and ever-growing threat to privacy. We confront a difficult problem of planning with, I think, very little idea of how to go about it.[7] Professor Countryman's remarks have prompted me to formulate one tentative approach to this important task, and I hope that they will have the same effect on others. As Professor Countryman says, the time for inquiry is overdue. We must begin the job now if the future is to be governed by our actions rather than our defaults.

---

[6] *See generally* A. WESTIN, PRIVACY AND FREEDOM (1967).

[7] *See generally* NAT'L ACADEMY OF SCIENCES, TECHNOLOGY: PROCESSES OF ASSESSMENT AND CHOICE (1969).

THE DIMINISHING RIGHT OF PRIVACY: A REJOINDER

VERN COUNTRYMAN

Professor Alschuler and I have even more common ground than he supposes, due to his overlooking my statement that "careful study of the contents of various compilations, and careful consideration of the justification therefor [by Congress], would be required before lines could be drawn." Thus, I did not "propose" that department stores be forbidden to use credit bureau files, but only that there was "room to doubt" their need for such use and that the common assumption that they had such a need had never yet been explored. And I certainly did not intend to, and do not believe I did, suggest that even the most vital public need for information would justify such odious practices as electronic surveillance, by official or private operators.

Still, there is a substantial area of disagreement. I view the existence of computerized dossiers in their present and prospective magnitude as a threat to privacy which will not, and in my view cannot, be effectively curbed by restrictions on access. I challenge the widespread assumption—in and out of Congress—that because they exist they must be allowed to continue to exist. I suggest, as a standard for Congressional inquiry that would test this assumption by provoking some pertinent questions not yet asked (and not as a standard for ongoing operations by some administrative agency, as Professor Alschuler interprets my proposal), "an actual need for a vital public purpose, rather than . . . a convenience or a comfort for any acceptable purpose." An inquiry based on such a standard would lead, in my judgment, to the conclusion that much of the present stock of dossiers is not at all necessary and must be eliminated because its use cannot be effectively controlled. Such an inquiry should also, by improving our understanding of the areas of actual need, make us better equipped to devise defensible and enforceable restrictions on access to the more manageable stock of compilations which would survive.

If this position opens me to charges of viewing technology and organization "as our villains," of confusing "the medium with the message" and of burning unprinted books, so be it. Professor Alschuler's alternative apparently is to do nothing about the proliferation of computerized personal dossiers, but to place complete reliance on imposing limitations on access to them. For reasons that I have already developed at some length, I do not believe that limitations can be

developed that will give adequate protection against technological raiding, illegal activity by government officials, or a change in policy by the limitation-imposer. Nothing that Professor Alschuler has to say allays my fears in this regard.

If I am "essentially backward-looking" and guilty of seeking "to recapture the era before the computerized personal dossier and the national data bank came into existence," or at least some segment of that era, I believe that Professor Alschuler is not sufficiently forward-looking to appreciate the dangers ahead. The incident of Judge Carswell illustrates what I mean. Both Professor Alschuler and I thought that blocking Judge Carswell's appointment to the Supreme Court served a vital public purpose. Since the FBI did not have a complete and accurate computerized dossier on Judge Carswell and its investigators were not as diligent as newspaper reporters, several highly relevant pieces of information about Judge Carswell were not unearthed until after his nomination was submitted to the Senate. It would have been more efficient—and it might have spared the President, the Senate and Judge Carswell himself considerable pain—if the FBI had been able to produce a complete and accurate dossier on Judge Carswell from its computers. If present trends continue, the FBI will be able to produce such dossiers on virtually all prospective nominees. In my view, it would be less damaging to our society to have Judge Carswell on the Supreme Court.

[EXCERPTS FROM THE UNIVERSITY OF ILLINOIS LAW FORUM, VOL. 1971, NO. 2]

Copyright 1972 by the Board of Trustees of the University of Illinois

PRIVACY AND GOVERNMENT INVESTIGATIONS†

*Senator Sam J. Ervin, Jr.**

SINCE THE DAWN of civil society, men have contended over the ways government exercises its investigative power as they have contended over the ways to reach heaven. Americans in the twentieth century offer no exception to this truth. Their concern is the greater because privacy is valued in our society as a hallmark of freedom. Yet recently it has been threatened or diminished in ways and for reasons that to some people seem beyond our challenge or our control.

There are those in our country who believe that to enforce the laws, government should investigate everything and there are those who believe that to preserve liberty, government should investigate nothing. There are those, and I count myself among them, who believe that government must have ample power to investigate and to gather information in order to govern, but who also believe that there are certain things which are none of the business of government. There are those, and I count myself among them, who believe that a free society must take some risks in order to remain free, but who also believe that, similarly, the individual under a government of laws must assume the risks and the legal consequences for his actions.

The glory of our constitutional system is that its authors set down for the ages the lessons learned about man's struggle to control governmental power. As we discuss the power of government to investigate and to monitor the activities of those it governs, we have ever before us certain fundamental principles governing the exercise and control of power over the individual in our society. It is those constitutional principles, designed to keep all men free in their minds and in their spirits, which I believe will see America through any crisis. If these principles are meticulously observed, I believe neither wars nor natural disasters, neither threats from beyond our borders nor threats from within, neither dissent nor rebellion, neither economic perils nor political instability will founder this nation.

In the crisis atmosphere in which government officials must frequently operate as they attempt to solve major social and economic

† *These remarks were originally delivered as a lecture in the Privacy and the Law Series at the University of Illinois College of Law, May 7, 1971.*

**United States Senator from North Carolina. B.A. 1917, University of North Carolina; LL.B. 1922, LL.D. 1951, Harvard University; LL.D. 1955, Western Carolina College.*

37-583 O - 74 - pt. 2 - 8

problems, there are some forces at work which often make it difficult to assure the proper balance between the needs of government and the freedom of the individual guaranteed by the Constitution. I want to stress that while we should be on guard against the adverse effects of these forces, I think that properly channeled, they may be counted among America's best hopes for creative progress.

One of these forces is the increasing demands on government for new and better services of all kinds. Another is the greater political awareness and activity on the part of citizens from every walk of life who want to have greater influence on their government and a larger role in helping to shape policy.

Another force is computer technology and the use of scientific methods of systems analysis which it encourages. In a study by the Constitutional Rights Subcommittee, we found that the increased use of government and private computer-based systems is making it vastly more economical to acquire and store information about people for reasons which should give Americans serious pause. It is creating not only an army of specialists in the information-processing field, but battalions of investigators and analysts specializing in seeking out and reporting derogatory information on individuals.[1] It is feeding the zeal of statistics collectors in government who claim they need information for research and who back their requests for data with the sanctions of criminal and civil law.[2]

There is another force affecting our privacy caused by the development of the behavioral sciences with their emphasis on analysis of man's behavior in society and organizations, their emphasis on what makes him think as he does and act as he does, and on what elements go to make up his personality. This wave of personality study has taken over government and private industry alike. In its name, many sophisticated questionnaires and pseudoscientific instruments such as personality tests and lie detectors have been developed to elicit personal information.[3]

The result of all this is that officials at every level of our national life who make decisions about people for limited purposes seem possessed by a desire to know the "total man" by gathering every possible

1. *See* Ervin, *The Computer and Individual Privacy*, 113 CONG. REC. 5898 (1967) (address before the American Management Association, on March 6, 1967); *see also* comments by Senator Ervin on computer abuses and suggested remedies, 115 *id.* 33576, 39114 (1969).

2. *See generally Hearings on S. 1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.*, 91st Cong., 1st Sess. (1969). Ervin, *Privacy, the Census and Federal Questionnaires*, 115 CONG. REC. 17718 (1969).

3. *See Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.* (1965); Remarks of Senator Ervin on S. 2156, A Bill To Protect Against Invasion of Privacy by Prohibiting Lie Detectors, 117 CONG. REC. S. 9870 (daily ed. June 24, 1971).

bit of information about him. The further result is that government and private computers and dossiers are filled to overflowing with the trivia of the daily lives of people. Although frequently meaningless, the trivia obtain in official reports of government agencies and credit companies an infallibility which can adversely affect a person's life and fortunes, and even his honor.[4]

Yet all of these forces are at work on agencies and organizations operating under laws meant, for the most part, for another era, less oriented to the need for total information and less in need of rapid analysis and cross-country transmission of data.

There have been many charges recently of illegal privacy invasion, especially about the surveillance practices of the Federal Bureau of Investigation. Many people equate the activities of that agency with those of the Army, whose broad program for data-gathering on civilian politics has been widely criticized and discussed recently. I believe they fail to realize the differences. The FBI, it is true, has very broad investigative powers, and along with other agencies its investigative reports frequently contain nothing but trivia. Its methods, along with those of other agencies, may need some ethical refurbishing. On the other hand, it is sometimes forgotten that, unlike the Army, the Bureau has been given legal responsibilities for investigating a great range of federal criminal laws, many of them vaguely worded. These include all of our espionage and security laws. They include the broad investigations demanded by the 1954 executive order which President Eisenhower issued requiring the FBI, the Civil Service Commission, and other agencies to investigate an individual's character, morals, emotional stability, and good judgment in order to determine if he might become a security risk.[5] So, if some are finding that in our computer age the investigative power of federal law enforcement officers should perhaps be better defined in writing, that is not necessarily the same as saying that the officers have been acting illegally.

While there may be misunderstanding on the part of some about the FBI, I do not agree with those who claim it is "political demagoguery" and "hysteria" to speak of violations of privacy and constitutional rights by government investigations. Indeed, I believe it is timely to do so if our fundamental freedoms are to be preserved.

I say this because it is clear to me from the complaints coming to Congress that the combination of executive branch politics and these

4. A.R. MILLER, THE ASSAULT ON PRIVACY 67-89 (1971); *Hearings on S. 823 and Fair Credit Reporting Before the Subcomm. on Financial Institutions of the Senate Comm. on Banking and Currency*, 91st Cong., 1st Sess. (1969); *Hearings on H.R. 16340 and Fair Credit Reporting Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency* (1970).

5. *Security Requirements for Government Employment*, Exec. Order No. 10,450, 3 C.F.R. 936 (1953), *as amended*, Exec. Order No. 10,550, 3 C.F.R. 200 (1954).

three social forces I have described has produced a novel claim in the executive branch to an inherent constitutional power to investigate people whose only crime is exercise of their first amendment freedoms.

This claim of investigative power is founded in the desire to predict violations of the law and to take preventive measures before there is any overt sign of intent to commit a crime. It is founded in a very human curiosity to know what people are thinking. The problem is that it clashes with the fundamental constitutional principle that what people are thinking is none of the business of government investigators. I believe that, unchecked, the exercise of such an inherent power can quickly give this nation the trappings of a police state.

The Subcommittee has discovered a number of instances of agencies who started out with a worthy purpose for investigating, but who, under the inherent power concept, went so far beyond what was needed in the way of information that the individual's privacy and right to due process of law are threatened by the very existence of the files the agencies collected.[6]

One massive investigative program pursued under this inherent power theory was the Army's civil disturbance prediction program which caused it to spy on thousands of Americans in order to try to predict when disturbances would occur which could not be controlled by local or state police power and when the President would be requested to supply military assistance.[7]

Concern about Army prying into civilian affairs has been expressed to Congress by people in every state of the Union. There has been special concern in Illinois because of the publicity given the surveillance activities of the 113th Military Intelligence agents.

It is the students of the law who because of their special knowledge of the Constitution can perhaps best understand the threats to liberty caused by the kind of Army surveillance, investigation, and data collection described recently before the Senate Constitutional Rights Subcommittee.[8]

I think it should be stated here that despite their failings, Army officials were not the chief focus of our investigation. For a number of years, the Subcommittee has received many complaints about excessive

6. *See generally* Remarks by Senator Ervin announcing hearings on computers and data banks and describing responses to Subcommittee survey of federal departments and agencies, 116 CONG. REC. 30797 (1970), 117 *id.* S. 985 (daily ed. Feb. 8, 1971).

7. For an account of developments in this investigation of the Army surveillance and data banks, together with relevant articles and texts of correspondence *see generally* 116 CONG. REC. 2225, 5496, 26327, 41751, 43944 (1970) (Remarks of Senator Ervin).

8. Pyle, *Conus Intelligence: The Army Watches Civilian Politics*, Washington Monthly, Jan. 1970; Pyle, *Conus Revisited, id.* July 1970. These articles also appear with remarks by Senator Ervin, 116 CONG. REC. 2225, 5496 (1970).

federal demands for personal information from people, about haphazard computerization, exchange and distribution of data without proper safeguards, and about data banks for storage of all kinds of extraneous information unrelated to the needs of the agency.

We initiated a survey of all departments to learn what laws and rules govern these data banks and computers and how they affect the privacy of the individual. One of our original reasons, therefore, for investigating the Army was to learn what computers and data banks the Department of Defense maintained on people. The Subcommittee has experienced considerable difficulty with many departments in obtaining frank answers to our inquiries, but the Army, it is safe to say, has been the least frank of all.

During our hearings on computers, data banks, and the Bill of Rights,[9] we learned that the Army has been assigned the work of a national police force. It had been given the task of spying upon American citizens who were exercising their first amendment freedoms. In pursuance of this mission, the Army technocrats put into use an arsenal of surveillance weapons and techniques. These included the products of personal observation of agents, as well as computers, microfilm data banks, video recorders, photographs, card files, and manual files.

Such a program was fraught with danger for the very freedoms which were designed to make the minds and spirits of all Americans free and which work to keep America a free society. It is those first amendment freedoms which are the most precious rights conferred upon us: the freedom to think one's own thoughts regardless of whether they are pleasing to government or not; the freedom to speak what one believes whether his speech is pleasing to the government or not; the freedom to associate with others of like mind to further ideas or policies which one believes beneficial to our country, whether such association is pleasing to government or not; the freedom to assemble peaceably with others and petition government for a redress of grievances; and the freedom to worship Almighty God according to the dictates of one's own conscience.

Notwithstanding these freedoms conferred by the Constitution, the Army spied upon people attending divine services in churches; it infiltrated religious organizations; and it placed large groups of Americans under surveillance when the only offense committed was to exercise their first amendment freedoms.

On one occasion 119 persons met together to protest certain poli-

9. See generally *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.*, 92d Cong., 1st Sess. (1971) [hereinafter cited as *1971 Hearings*]. Prepared statements of witnesses who testified on the Army program are also collected in *Uncle Sam Is Watching You: Highlights from the Hearings of the Senate Subcommittee on Constitutional Rights*, Public Affairs Press (1971).

cies of government with which they disagreed. Their meeting was entirely peaceable and nonviolent. Yet it turned out that only sixty-seven persons were protestors and that a very large number were military and law enforcement agents ordered, along with the press, to attend this meeting, to take pictures of the persons present, and to tape the speeches which were made. One military intelligence agent in attendance said that the speeches were wholly nonviolent in nature but that they could not tape them because of the noise of five Army helicopters which flew directly over the meeting during its continuance, spying upon the 119 people from above.[10]

The Subcommittee was told that with very little in the way of guidelines for their activities, the Army maintained computerized microfilm and manual files on membership, ideology, programs, and practices of virtually every activist political group in the country.[11]

These included not only violence-prone organizations, but also such nonviolent groups as the American Friends Service Committee, the Southern Christian Leadership Conference, Clergy and Laymen on the War in Vietnam, the American Civil Liberties Union, the Women's Fight for Peace, and the National Association for the Advancement of Colored People. Groups as diverse as the Ku Klux Klan, the Communist Party, the Students for Democratic Society, and Businessmen Against Vietnam were covered. Intelligence agents testified that they were ordered to infiltrate groups protesting various government policies.[12] They joined peace groups, monitored mothers' meetings, attended community poverty board meetings, and reported on campus events, activities, and classes.

Now the military did not just collect all of this information and keep it secret. The Army shared their blacklists with many federal, state, and local agencies.[13] They had their analysts study the data and try to codify it in order to put it into computers and microfilm data banks. One intelligence analyst told the Subcommittee how the Counter Intelligence Analysis Branch received reports on persons often obtained covertly by Army agents and FBI informants. These reports contained detailed information on finances, sexual activities, personal beliefs, and associations of famous people, as well as anonymous Americans. They contained detailed background investigations on anti-war protestors arrested by local police for misdemeanor offenses, as well as

10. *1971 Hearings* 315 (testimony of Laurence Lane).
11. *Id.* 147 (testimony of Christopher N. Pyle).
12. *Id.* at 244.
13. For a list of the federal agencies requested to furnish information to the Army see Appendix B to the *Department of the Army Civil Disturbance Information Collection Plan of May 1968, 1971 Hearings* pt. 2. The text also appears in 117 CONG. REC. S. 2290 (daily ed. March 2, 1971) (remarks of Senator Bayh). For the Army distribution list for its own data and the number of copies each agency received see Appendix D to the *Information Collection Plan, supra.*

reports on speeches in all of our cities.

To make the difficult decisions about what category a person belonged in, the analyst was required to examine these reports and then resort to a special intelligence code. He had to apply various number combinations which indicated a person's beliefs or status. For instance, 134.295 indicated that a person was a non-Communist, while 135.295—a difference of one digit—indicated Communist Party membership or advocacy of Communism. We were told that since many of these persons were young people with no political philosophy and no organized memberships, the analyst had nothing to go on but some political utterances. On the basis of these, he sometimes chose a designation arbitrarily in doubtful cases.[14]

Despite all of the information-gathering, the computers, and the data banking, the Subcommittee has yet to be told why this was thought to be useful. I found no instance when a doughboy sniped on in Detroit would have found this information useful. In fact, the Deputy Chief of Staff of the Army Intelligence Command didn't even know there was a computer program at Fort Holabird. The Subcommittee was first told informally that there were no computers; then, that there was one, but that it had been disconnected for this program; then, that there were a few more computers that the Defense Department had forgotten about or not known about.

On the basis of all the confusion displayed by these officials, it became clear to me that computers have far too much privacy in the Army as well as elsewhere in the executive branch.

The Subcommittee has been unable so far to discover exactly who ordered this surveillance, how useful the information was, how extensive the program was, and how many churches, universities, and communities were spied on. The Department of Defense in their testimony admitted little more than we had been told by the press, former agents, and other sources. This is despite our continuous requests for pertinent documents and for the testimony of the generals and officers with most knowledge about the program.[15]

I do not, however, believe the Army proceeded on its course alone or unauthorized. Someone tried to make prophets out of some G.I.s serving out their tour of military duty.

The Army was finally given a Civil Disturbance Plan to follow for

14. *1971 Hearings* 248, 260 (Stein testimony).

15. For an account of the Subcommittee requests for testimony of knowledgeable civilian and military officials, for declassification of pertinent documents and delivery of others *see generally* the exchange of correspondence between Senator Ervin and Defense Department officials between July 29, 1970 and Dec. 4, 1971, *1971 Hearings* pt. 2 (App.). For a discussion of the constitutional issues and a list of the Defense Department's reasons for their withholdings and delays see Ervin, *Secrecy in a Free Society*, 213 NATION 454 (1971).

its activities in January 1968.[16] They were told to watch people in the civil rights movement, the anti-draft movement, and in labor disputes. This "Plan" was supplemented in February 1968 by a document setting forth the intelligence interest of the Army.[17] It shows that all this information was to be collected despite the recognition that the majority of civilians were law abiding. The "Intelligence Annex (B)" said that "although the majority of anti-war protestors appear reluctant, for moral, practical, or legal reasons, to engage in public demonstrations of a nature which violates existing laws, there is a significant minority of professional agitators and young students who advocate either violent action or so-called disobedience." Then the Plan said that, while it recognized that the majority of the people who participate in these activities were loyal Americans, there was an apprehension that they might be under the direction of some foreign groups and might not know their own minds. It stated that notwithstanding the fact that most of the black population abhors violence, these people might still be made dangerous to society by the militants.

Another document supplementing the January Plan was the Civil Disturbance Information Collection Plan of May 1968, which shows that the Army agents and commanders were to gather information about "threshold activity" and pre-civil disturbance matters. Other federal law agencies and military departments were asked to supply similar information. They were told to find out "the identity of newspapers, radio or television stations, and the names of prominent persons friendly with the leaders of the disturbance and who were sympathetic to their plans. Whether any would be present, participating, and how." They were told to find out the probable categories and identification of persons and groups who would create or participate in a civil disturbance, the estimated number of persons who would be involved as participants and as observers, and the overt and behind the scenes leaders' identity. The Army wanted to know about protests of the minority community to conditions in slum areas such as de facto segregation in unions, housing, and schools, and such as local merchants and landlords overcharging for housing and goods. They wanted to know about efforts by minority groups to upset the balance of power and the political system.

They asked about the "high command" of dissident groups, their organizational charts, rosters of key personnel, and the numbers of active members; the breakdown of membership by ethnic group, age, economic status, education, criminal record, and biographic data on key members.

16. *1971 Hearings* 398, 419. As of Dec. 1971, neither the basic Jan. 1968 Plan nor the Army's new 1970 Civil Disturbance Plan had been declassified.

17. *1971 Hearings* pt. 2 (App.). Annex B (Intelligence) to Dept. of the Army Civil Disturbance Plan (Feb. 1, 1968, unpublished).

They wanted information on "evidence of or attempts by subversive organizations to penetrate and control civil rights or military organizations composed primarily of non-whites."

They wanted to know the "aims and activities of groups attempting to create, prolong, or aggravate racial tensions, such as CORE, NAACP, SNCC, National States Rights Party, Southern Christian Leadership Conference, and the Council of Federated Organizations." As a separate category, they even wanted information about the women members of such groups.

With such a broad mandate, it is small wonder that zealous commanders and industrious agents felt that they had to scoop up everything of possible interest in their reports and that they would feel required to keep under surveillance every politically active citizen and group exercising first amendment freedoms.[18]

I asked the Assistant Secretary of Defense, Mr. Froehlke, if he thought that existence of this information system would not have a debilitating effect upon the exercise of the constitutional rights of free speech and assembly by many of our politically aware citizens. He replied that he didn't think there was any violation of the first amendment.[19]

"We maintain there was no illegal activity. We think we maintain there was inappropriate activity," he said. He admitted that some of the Army's activities didn't "make much sense" from the management point of view, but he didn't know whether he would call them "illegal."[20] Merely watching someone, he testified, does not violate any constitutional rights, unless there was some "specific evidence that someone was deterred." If it was unknown, it was argued, the man wouldn't know it, so it could hardly deter his activities. Of course, it must be noted that the Army did more than "watch." They took notes, made dossiers, photographed, and tape recorded.

In my opinion, the argument that blacklists and surveillance programs which are unknown to the public can't hurt anyone is specious. Such an argument is common in government, but it flies in the face of the principle of open government which is the keystone of our Constitution. It denies the basic right of the people to full information about the activities and programs of their government. This is the constitu-

18. *1971 Hearings* 421, 422 (testimony of Assistant Secretary of Defense Robert F. Froehlke).

19. *Id.* at 430.

20. *Id.* 431. See also *id.* at 385 (Froehlke testimony):

> It is worthy of note that none of the activities referred to above were prohibited by Federal or State law . . . . Since no use of civil disturbance information was made or intended to be made that would result in any action to the prejudice of any individual or organization, it is difficult to perceive how the constitutional rights or even the right of privacy could be impinged by the collection of such information.

tional principle which was implemented recently in the Freedom of Information Act[21] and which is reflected in many other statutes requiring disclosure and full reports of government programs. The Froehlke argument assumes that people will not find out about illegal or unconstitutional programs. If Mr. Froehlke needed more proof that unconstitutional programs cannot be hidden from the people for very long, he has only to look at the history of the Army's civil disturbance program and he has only to consider the shock and dismay of the American people which they expressed to Congress as the full scope of this program was made known to them by former agents and by the press.

Some executive branch officials have not yet discovered the truth of Abraham Lincoln's observation, for it is clear from their arguments on this matter that they think the government can fool all the people all of the time. Secretary of Defense Laird and the Army sent word that the intelligence-gathering on civilians was being cut back and that the computers, in effect, were unplugged. He said the Army would henceforth rely on the Department of Justice for civil disturbance information.[22]

In view of that assertion, I asked the Attorney General, as chief legal officer of the Government, for his opinion on the constitutionality of the collection of information by the Army or other executive departments on people who were not suspected of breaking any laws but who were merely exercising their first amendment rights.[23]

He delegated this task to the Assistant Attorney General, Mr. Rehnquist, who told the Subcommittee that he didn't think it would stifle first amendment freedoms to place such persons under surveillance.[24] He said that "[i]t may have a collateral effect such as that but certainly during the time the Army was doing things of this nature, and apparently it was fairly generally known that it was doing these things, it didn't prevent two hundred fifty thousand people from coming to Washington on at least one or two occasions to protest the war policies of the President."

He also told us that while there might be " 'isolated abuses' of the investigative function, they were not unconstitutional."[25]

He further stated that he knew of no authoritative decision holding that it was unconstitutional to collect information which is not le-

21. 5 U.S.C. § 552 (1970).

22. *1971 Hearings* 394. *But cf. id.* at 436 (Froehlke testimony): "Nevertheless, experience has taught me that I cannot tell you that under no circumstances should the Army ever observe non-DOD-affiliated civilians. I think under certain extreme circumstances the Army might again have to, and that is the criteria we are talking about."

23. *Id.* at 571. The Subcommittee letter to the Attorney General also appears with remarks by Senator Ervin, 116 CONG. REC. 26327 (1970).

24. *1971 Hearings* 620.

25. *Id.* at 602, 603.

gitimately related to the statutory or constitutional authority of the executive branch to enforce the laws.[26] It was his contention that there is no constitutional rights violation by government investigation and data-gathering unless a government sanction is involved.[27] My own suspicion of an unchecked executive branch investigative power was borne out during his testimony when he advanced the amazing theory that "self-discipline on the part of the executive branch will provide an answer to virtually all of the legitimate complaints against excesses of information-gathering."[28]

Mr. Rehnquist and other Justice Department officials bandied about a vague theory of preventive law enforcement which justifies surveillance.[29] They cited article III, section 3 of the Constitution as the "source of the duty of the President to oversee the faithful execution of the laws and thereby exercise implicit power to investigate, prosecute, and prevent violation of the Federal law." As another source of information-gathering in the executive branch, they cited article IV, section 4, providing that the United States shall guarantee every state a "Republican Form of Government," and on application of the legislature, or of the executive, [shall protect each] "against domestic Violence."[30] They cited an 80-year old Supreme Court decision, *In re Neagle*,[31] involving a shoot-out between two judges. They cited statutes on the federal role in civil disturbances.[32] But they conveniently ignored the Bill of Rights.

Rather, they, like the Army, laid claim to a constitutional power of investigation for purposes of preventive law enforcement which, given the scope of federal criminal and civil laws, if carried to its logical extremes, could justify surveillance of any citizen for almost any purpose whatsoever.

26. *Id.* at 602.
27. *Id.* at 620.
28. *Id.* at 603.
29. *Id.* at 602.
30. *Id.* at 599.
31. *In re Neagle*, 135 U.S. 1, 10 S. Ct. 658 (1890).
32. 10 U.S.C. §§ 331-33 (1970). Under U.S. CONST. art. 1, § 4, and 10 U.S.C. §§ 331-33 (1970), the President has authority to use the armed forces for these purposes:

1. To suppress rebellion, insurrection, or domestic violence, which obstructs the execution of the laws of the United States, or impedes the course of justice under those laws.
2. To suppress insurrection against a state if state authorities so request.
3. To suppress insurrection or domestic violence in a state, which so hinders the execution of federal or state laws within the state as to deprive "any part or class of its people . . . of a right named in the Constitution and secured by law" if the constitutional authorities of the state (a) are unable, (b) fail, or (c) refuse to protect that right.

10 U.S.C. § 334 (1970) provides that whenever the President considers it necessary to use the armed forces under §§ 331-33, "he shall, by proclamation, immediately order the insurgents to disperse and retire peaceably to their abodes within a limited time."

I must take issue with the Department of Justice officials on all of these counts, for I believe they fail to understand the relationship between constitutional liberty and the government's claim to a power to investigate people in order to determine future behavior.

First, contrary to the opinion offered by the Assistant Attorney General, recent events have shown that there is indeed a need for strict legislation in this area of the law. "Self-discipline" is not enough. It has not prevented the Army spying on civilians; it has not precluded the Census Bureau and other information-gathering agencies from harassing people with broad questionnaires. It has not prevented the continuing inquiries into the most private lives and beliefs of federal employees and applicants. It did not stop the Secret Service from computerizing people who write letters about their grievances to high government officials, who are professional gate-crashers, and who make remarks embarrassing to high government officials at home or abroad. "Self-discipline" does not help the wives of applicants for FHA loans when they are compelled to disclose their birth control practices and confidential advice from their doctors. Nor has "self-discipline" prevented all the other programs from violating personal privacy.

So I believe there must be new laws geared to the computer age, with specific guidelines for gathering personal data and with carefully drawn controls on the use, exchange, and protection of such information. Furthermore, I believe that some provision must be made to provide the individual access to government records about him and the chance to assure the accuracy of such information.[33]

Secondly, contrary to the opinion of lawyers at the Justice Department, I have found that the courts have long been active in this area, and I predict that they will be even more active if the executive branch continues to try to make prophets of its civil servants and if it continues in its present claim to an inherent power to make inquiries in the course of trying to predict the future behavior, attitudes, and beliefs of law-abiding Americans. For instance, the United States Supreme Court will soon consider the case of *Laird v. Tatum*,[34] a suit challenging the

33. For an excellent discussion of the constitutional, legal, and philosophical problems involved in such an effort for one area of information-gathering *see generally Security and Privacy Considerations in Criminal History Information Systems*, Technical Rep. No. 2, July 1970, by Project SEARCH, California Crime Technological Research Foundation, funded by the Law Enforcement Assistance Administration, Department of Justice. Related to this issue is S. 2546, A Bill To Facilitate and Regulate the Exchange of Criminal Justice Information Systems, introduced by Senator Roman Hruska Sept. 20, 1971. 117 CONG. REC. 14563 (daily ed. Sept. 20, 1971). Also pertinent is the testimony of Richard Velde of the Law Enforcement Assistance Administration on the use of information and intelligence systems by criminal justice agencies. *1971 Hearings* 605, 849, and testimony of FBI officials concerning the National Crime Information Center. *Id.* 914.

34. 444 F.2d 947 (D.C. Cir. 1971), *cert. granted*, No. 71-288, 1971 Term (40 U.S.L.W. 3238).

Army program. Dismissed by the district court as not presenting constitutional rights issues, the case is defended by the Government with the claim that the threat of surveillance is not sufficient to invoke the judicial process and, furthermore, that the plaintiffs have not demonstrated a personal stake in the outcome of the controversy. According to the Justice Department, the record "presents only abstract legal issues involving, at best, the speculative impairment of constitutional rights."[35]

Many people, like the Assistant Attorney General, seem to think this is new legal ground which must be pioneered. These officials have overlooked the significance of numerous court decisions bearing on privacy and the investigative power of government.

On the basis of my study of the decisions, I believe this case law was correctly summarized by Professor Bernard Schwartz in terms which should be brought to the attention of all government agencies. He writes:

> Of course, government may deal at any time with threats to its security expressed in acts. Where speech, association and other First Amendment rights are involved, on the other hand, the power of investigation should be no more far-reaching than that of legislation. In our system, authority over a subject matter involving speech, press, assembly, and the like must not go beyond the power to do that which is essential to be done in protection against a public danger. Civil liberties may not be abridged by investigatory authority merely in order to determine whether they should be abridged.[36]

From reports received by the Constitutional Rights Subcommittee, I think not only the Army investigators, but other federal and local agents are too often engaged in investigations of people merely to determine if they should be investigated or if dossiers should be kept on them. Under Professor Schwartz's test, such practices, wherever they occur, violate first amendment rights.

Thirdly, unlike Administration officials, I think there are serious constitutional rights violations in these surveillance programs.

I have found three Supreme Court decisions in particular which provide a point of departure for courts and legislatures seeking guidance in setting controls on unwarranted information-gathering and data banking. I recommend these decisions to officials in the executive branch who assert a broad claim to investigative power.

The first case is *United States v. Rumely,* decided in 1953.[37] In that case, the accused was the secretary of an organization which, among other things, engaged in the sale of books of a political nature.

35. *Id.* Petitioner's Brief for Certiorari at 10 n.4.

36. B. SCHWARTZ, 1 COMMENTARY ON THE CONSTITUTION OF THE UNITED STATES: POWERS OF GOVERNMENT 140 (1963).

37. 345 U.S. 41, 73 S. St. 543 (1953).

The House Select Committee on Lobbying had called on him to disclose the names of those who made bulk purchases of those books for further distribution. He refused to furnish the names and was convicted under a statute providing penalties for refusing to give testimony or to produce relevant papers upon any matter under congressional inquiry. The Committee claimed authority to demand this under the power, stated in their resolution, to investigate all lobbying activities intended to influence, encourage, or promote legislation.

Justice Frankfurter delivered the opinion of the Court, holding that the accused was not required to deliver the names on the ground that the authorizing resolution restricted the Committee to a study of lobbying activities which were carried on directly with members of Congress and could not extend to a person's effort to influence legislation through the means of books and periodicals. With this as an alternative ground for decision, the Court did not have to reach the constitutional issue. However, the Justice made the significant observation: "Surely it cannot be denied that giving the scope to the resolution for which the Government contends, that is, deriving from it the power to inquire into all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiations of influence which they may exert upon the ultimate legislative process, raises doubts of constitutionality in view of the prohibition of the First Amendment."[38]

Justice Douglas wrote a concurring opinion in which he said that he was compelled to face the constitutional issue that this involved the grant of power to the Committee. He pointed out, in an able opinion with which I thoroughly agree, that the resolution did not give the Committee the power it claimed but that it was unconstitutional as a violation of the first amendment guarantee of the freedom of press and speech. He recognized that no legal sanction was involved here but felt that it could be the beginning of surveillance of the press. Under such a rule, he noted, the spectre of a government agent will look over the shoulder of everyone who reads, and the subtle imponderable pressures of the orthodox will lay hold. "Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press. Congress could not do this by law. The power of investigation is also limited. Inquiry into personal and private affairs is precluded. . . . And so is any matter in respect to which no valid legislation could be had."[39]

Therefore, since Congress could not by law require of Rumely what the House demanded, it could not take the first step in an inquiry ending in fine or imprisonment.

38. *Id.* at 46, 73 S. Ct. at 546.
39. *Id.* at 58, 73 S. Ct. at 551-52 (citations omitted).

The second opinion which I think is very illuminating on this subject is the case of *NAACP v. Alabama*.[40] There the question was presented whether Alabama, consistent with the due process clause of the fourteenth amendment, could compel the petitioners to reveal to the state's attorney general the names and addresses of all of its Alabama members and "agents" without regard to their positions or functions in the Association. Justice Harlan wrote the unanimous opinion of the Court, holding that Alabama was precluded by the due process clause of the fourteenth amendment, which, of course, made the first amendment applicable to the states, from requiring this information. He said, and I commend this to the Department of Justice: "It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."[41]

The Justice noted that inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs. The Court held that the immunity from state scrutiny of membership lists which the Association claimed was so related to the right of the members to pursue their lawful private interest and to associate freely with others in so doing as to come within the protection of the fourteenth amendment. It held that Alabama had failed to make a showing of overriding valid interest in possession of such information and that judgment of the Alabama court punishing the respondent for contempt of court was invalid under the Constitution.[42] It is a natural extension of these decisions to say that, for example, the federal government can't go out and observe people exercising their first amendment rights and then take steps which have the effect of stifling their willingness to continue in the exercise of their first amendment rights.

What inquiries and investigations Congress and the states may not undertake under the Constitution, certainly the executive branch has no inherent power to undertake.

There is another opinion which I think sums up the constitutional law in this field very well. This is the dissenting opinion of Justice Harlan, joined by Justices Frankfurter, Clark, and Whittaker, in the case of *Shelton v. Tucker*.[43] It is in harmony with the *Rumely* and *NAACP* cases, although it differs on conclusions of fact. In the *Shelton* case, the State of Arkansas required every teacher, as a condition of employment or continued employment, to answer a questionnaire requiring among

40. 357 U.S. 449, 78 S. Ct. 1163 (1958).
41. *Id.* at 460, 78 S. Ct. at 1171.
42. *Id.* at 466, 78 S. Ct. at 1174.
43. 364 U.S. 479, 81 S. Ct. 247 (1960).

other things the name of every organization to which they had belonged or contributed during the preceding five years. The Supreme Court held that the statute interfered with associational privacy and went beyond legitimate inquiry for determining fitness. Justice Harlan in his dissent said in summarizing the law concerning rights under the first amendment, as made applicable to the states by the fourteenth amendment:

> Where official action is claimed to invade these rights, the controlling inquiry is whether such action is justifiable on the basis of a superior governmental interest to which such individual rights must yield. When the action complained of pertains to the realm of investigation, our inquiry has a double aspect; first, whether the investigation relates to a legitimate governmental purpose; second, whether, judged in the light of that purpose, the questioned action has subtantial relevance thereto.[44]

Judged by the test stated by Justice Harlan, it is clear to me that the Army's investigations of civilians had no substantial relevance to the duty of the military to know about roads, bridges, and major facilities, and to maintain men and equipment in readiness to assist in quelling rebellions and violence in those rare instances when local authorities could not maintain order.

The test of Justice Harlan could be applied to any government program for investigation, surveillance, and dossier-building on private citizens. Such practices should be tested by Congress and the legislatures not only for their relevance to a governmental purpose but for which agency of government should be assigned the investigative functions.

During 1967 and 1968, violent mobs burned and pillaged in some of our cities in numbers which disabled local officers to maintain order or enforce laws, and President Johnson dispatched the armed forces to those cities to suppress this domestic violence. He acted within the limits of his constitutional and statutory authority in so doing, but he and other civilian officials did not stop with using the armed forces to suppress violence. They assigned the Army the task of collecting information which would enable the President to predict when and where civilians might engage in domestic violence. It was certainly not the duty of the Army to engage in investigation of civilians for law enforcement purposes. It was engaged in programs which, if authorized at all, were more suitable for the Department of Justice and local law enforcement agencies. However I do not believe it has yet been demonstrated that this type of investigation and surveliance is necessary for any governmental purpose.

The fourth major disagreement I have with the Department of

44. *Id.* at 497-98, 81 S. Ct. at 257.

Justice and the Department of Defense is closely related to the third. This is over the issue whether or not their surveillance activities have a "chilling" effect on first amendment freedoms. Administration officials say there is no such effect. Of course, this is the most self-serving viewpoint possible for any official who wants to have unlimited power to gather information on people in order to do his job. How do you prove that people have been intimidated? You cannot, until it is too late. How do you know when a society has lost the life-giving sources of new ideas, of legitimate criticism, of intellectual and philosophical richness? The answer is that you cannot know until it is almost too late to recapture these qualities.

The Justice Department says it requires "sanctions" before it can find a constitutional rights violation in the collection of intelligence information. There are two answers to this "sanction" argument. First, files such as the Army had and shared may well be checked for employment, security clearances, or other purposes, and decisions made or impressions gained which the individual never knows about. Secondly, as frequently happens with the federal bureaucracy, the Department ignores the vagaries of the human spirit. It forgets the psychological sanction which may be imposed or threatened by the very knowledge of such executive branch excursions into constitutionally protected areas.

The first amendment is not so much for the brave. It is also for the weak of heart or those who are placed in such economically vulnerable positions that they cannot afford to risk the sanctions which may accompany legitimate criticism of government or unpopular opinions.

Congress has a great deal of evidence of such psychological pressures and subtle sanctions. Many people have written about their own reactions to the Army and other investigative programs. For instance, I received such a letter from an author who wrote the President about the Kent State matter. In reply he received some mimeographed pages defining Administration policies in Southeast Asia. He writes that he started to respond critically to this material but stopped because he could not be sure that he would not be put on a blacklist which could be used against him in the future.

This letter and many others like it provide the best answer I can give to the executive branch. They illustrate the one prophecy which I feel qualified to make today because it is based on centuries of historical fact. That is, a quiet America will not be a free America. Rather, it will be a spiritually lifeless America. For that reason I believe that this claim of an inherent executive branch power of investigation and surveillance on the basis of people's beliefs and attitudes may be more of a threat to our internal security than any enemies beyond our borders.

37-583 O - 74 - pt. 2 - 9

[EXCERPTS FROM THE UNIVERSITY OF ILLINOIS LAW FORUM, VOL. 1971, NO. 2]

Copyright 1972 by the Board of Trustees of the University of Illinois

THE DOSSIER SOCIETY†

*Arthur R. Miller**

IN RECENT YEARS there has been a growing public awareness of the effects certain data-gathering activities and applications of information technology may have on individual and commercial privacy. At times the debate has been conducted in emotional terms. For example, many people, myself included I must confess, have voiced the fear that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, and our associations are bared to the most casual observer.[1]

A brief recital of some of the blessings and blasphemies of the new technology makes the computer-privacy dilemma abundantly clear. In various medical centers, doctors are using computers to monitor physiological changes in the bodies of heart patients in the hope of isolating those alterations in body chemistry that precede a heart attack. The quest, of course, is to provide an "early warning system" so that treatment is not delayed until the actual heart attack has rendered the patient moribund for all practical purposes. Other plans include providing everyone with a number at birth to identify them for tax, banking, education, social security, and draft purposes. This would be done in conjunction with the computerization of a wide range of records. The goal is to eliminate much of the existing multiplicity in record-keeping, and at the same time expedite the business of society. Long range goals include developing a checkless, cashless economy, improving the informational bases available for rational planning, providing better services to people, and promoting the equitable allocation of society's resources. We may even see the day when if a person falls ill while away from home, a local doctor can use this identification number to retrieve the patient's medical history and drug reactions from a central data bank.

† *These remarks were originally delivered as a lecture in the Privacy and the Law series at the University of Illinois College of Law, March 25, 1971.*

* *Professor of Law, University of Michigan. A.B. 1955, University of Rochester; LL.B., 1958, Harvard University.*

The author has more fully explored the subject matter of his address in A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971), *and* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969).

1. Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC, Nov. 1967, at 53-57.

On the opposite side of the ledger, the same electronic sensors that can warn us of an impending heart attack might be used to locate us, track our movements, and measure our emotions and thoughts. Experiments already are underway in the field of telemetering and significant breakthroughs are on the horizon. Similarly, the identification number given us at birth might become a leash around our necks and make us the object of constant monitoring, making credible the fear of the much fabled womb-to-tomb dossier. Finally, the administrative conveniences provided by the high degree of information centralization made possible through the widescale use of computers gives those who control the recordation and preservation of personal data a degree of power over us that is unprecedented and subject to abuse.[2]

Close scrutiny and evaluation of the implications of data technology and information systems on individual privacy are especially appropriate at this time because of the clarion in all quarters for the establishment of governmental and private data centers. For example, the United States Office of Education is supporting a migrant worker children data bank, the Department of Housing and Urban Development is sponsoring computerized municipal information systems and building files on housing loan applicants (with particular attention given to those who are ineligible), and President Nixon's welfare reform proposal (the Family Assistance and Manpower Training Acts) will give the Department of Health, Education and Welfare authority to exchange individualized data with state welfare agencies and lead to the establishment of a national job applicant data bank. In other areas, we are seeing the emergence of criminal intelligence data centers, such as the Federal Bureau of Investigation's National Crime Information Center (NCIC), and computer based credit rating services. As we look to the future, there is no doubt that the hypnotic attraction of digital record-keeping will continue to envelope our universities, corporations, hospitals, and banks.

Indeed, I believe that Americans today are scrutinized, watched, counted, recorded, and questioned by more governmental agencies, social scientists, and law enforcement officials than at any other time in our history. Whether he knows it or not, each time a citizen files a tax return, applies for life insurance or a credit card, seeks government benefits, or interviews for a job, a dossier is opened under his name and his informational profile is sketched. It has now reached the point at which whenever we travel on a commercial airline, reserve a room at one of the national hotel chains, or rent a car we are likely to leave distinctive electronic tracks in the memory of a computer—tracks that can tell a great deal about our activities, habits, and associations when collated and analyzed. Few people seem to appreciate the fact that

2. Dombrowski v. Pfister, 380 U.S. 479, 487, 85 S. Ct. 1116, 1121 (1965).

modern technology is capable of monitoring, centralizing, and evaluating these electronic entries—no matter how numerous and scattered they may be.

Federal agencies and private companies are using computers and microfilm technology to collect, store, and exchange information about the activities of private citizens to an astounding degree. Rarely does a week go by without the existence of some new data bank being disclosed. During the past year we have read of the Department of Housing and Urban Development's Adverse Information File, the National Science Foundation's data bank on scientists, the Customs Bureau's computerized data bank on "suspects," the Civil Service Commission's "investigative" and "security" files, the Justice Department's intelligence bank run by that organization's civil disturbance group, the fact that files on 2.6 million individuals are maintained by the Department of Transportation's National Driver Register Service, the Secret Service's dossiers on "undesirables," "activists," and "malcontents," and the surveillance activities of the United States Army. These are only some of the federal government's data banks that have been brought to light; even now only the tip of the iceberg may be visible.

By and large, these data gathering activities are well intended efforts to achieve socially desirable objectives. For example, in the law enforcement field, file-building is necessary to combat organized crime and restore "Law and Order." In a similar vein, the FBI and the Army can justify their intelligence activities in terms of combating subversion or quelling campus disruptions and riots in our urban centers by knowing who to watch or seize in times of strife. As to the information activities of credit grantors, private investigators, and insurance companies, which involve considerable snooping into an individual's private life, it simply is good business to know as much as possible about a man before you lend him money, employ him, or insure his life.

But there is a negative side to these mushrooming data banks—particularly those that bear the imprimatur of a governmental organization. Consider the information practices of the United States Army. Early last year it was revealed that for some time Army intelligence units were systematically keeping watch on the *lawful* political activity of a number of groups and preparing "incident" reports and dossiers on individuals engaging in a wide range of *legal* protests. It must be emphasized that this monitoring not only covered society's "crazies" but included such nonviolent organizations as the NAACP, the ACLU, the Southern Christian Leadership Conference, and the Women Strike for Peace, and allegedly extended to newsmen, congressmen, and a former governor who is now a federal judge.

Although there is considerable justification for certain types of information collection that are directly relevant to the Army's duties, the

development of dossiers on people pursuing lawful social and political activities bears little relationship to the function of the military—even to its function during periods of social unrest. This is especially true when many of those being scrutinized are extremely unlikely to be involved in riotous conduct, and the selection of suspects seems to be governed by an incredibly simplistic these-are-the-good-guys-and-those-are-the-bad-guys approach. Not only is the Army's file-building difficult to justify, but it appears to have been undertaken without sufficient appreciation of the fact that the creation and exposure of dossiers on people who are politically active could deter them from exercising their right to assemble, speak freely, or petition the government.

The development of a number of other information systems in the law enforcement arena magnifies both the threat to personal privacy and the potential "chilling effect" of informational surveillance. The FBI's constantly expanding National Crime Information Center (prominently featured on the television series, "The FBI") provides state and city police forces with immediate access to computerized files on many people. Although it currently only contains data on fugitives and stolen property, plans are being formulated to add arrest records and other types of information to the FBI system. Moreover, NCIC is the keystone of an emerging information network that will tie together the nation's law enforcement information centers. By the end of 1969, the Crime Information Center reportedly was already exchanging data with state and local police agencies in every state except Alaska. State and local law enforcement surveillance systems also are becoming increasingly sophisticated—several with the aid of funding from the federal government under the Law Enforcement Assistance Administration program. New York already has the essential features of a network built around a single computer center designed to store information for state and local agencies and permit them to retrieve data through terminals placed throughout the state. An Ohio system allows 38 agencies to share its computerized information and is connected both to NCIC and the Ohio State Highway Patrol computer center; plans are underway to tie it to comparable systems in Kentucky and Indiana.

If a citizen knows that his conduct and associations are being put "on file," and he knows that there is some possibility that the information might be used to harass or injure him, he may become more concerned about the possible content of that file and less willing to "stick his neck out" in pursuit of his constitutional rights. The effect may be (to paraphrase a thought expressed by Justice Brennan in an analogous context) to encourage Americans to keep their mouths shut on all occasions.[3]

3. Lopez v. United States, 373 U.S. 427, 450, 83 S. Ct. 1381, 1393-94 (1963) (dissenting opinion).

If we really take our constitutional guarantees seriously, we cannot afford to stand by and allow them to be debilitated by this type of coercion. Claims of governmental efficiency or the war against crime and subversion must not be allowed to justify every demand for gathering personal data. Because of the potential development of a "record prison" mentality, no one should be surprised if some suggest that today's surveillance efforts contain the seeds of the much dreaded police state or a return to McCarthyism. Nor is it sufficient that governmental agencies assure us that surveillance and file-building are not being engaged in for repressive purposes. Nineteen eighty-four is a state of mind; for many people, the appearance of repression may have the impact of reality.

To prevent any doubt on the point, I personally do not oppose information systems or computerization of data. It strikes me as foolish to prevent the use of a modern technology to carry out important governmental and nongovernmental operations simply because it might be abused. This is especially true in our complex, urbanized society and mass economy, which desperately need data for sound national planning. We cannot turn the hands on the clock back. But this does not justify inaction. Even now we should recognize the strong similarity between the difficulties that gave rise to the multifaceted regulation of airlines, automobiles, railroads, radio, and television and the problems that already are generating pressure for the comprehensive regulation of data banks and computer communications.

What is necessary at this time is the development of a framework for the protection of the public and the superimposition of that framework on information practices at an early date to minimize misuse of an otherwise socially desirable instrument. The problem of striking a balance between democracy and technology has been a frequent and manageable chore in the past and the nation's policy makers should not shrink from the task in this context.

Let us turn now to the particular tensions between contemporary data activities and privacy. Until recently, informational privacy has been relatively easy to protect for a number of reasons: (1) large quantities of information about individuals have not been available; (2) the available information generally has been decentralized; (3) the available information has been relatively superficial; (4) access to information has been difficult to secure; (5) people in a highly mobile society are difficult to keep track of; and (6) most people were unable to interpret and infer revealing information from data.

But these protections were part of a bygone era and are alien to our technologically based society. The testimony elicited before several committees of the United States Congress that have held hearings on privacy presents an astounding, and disheartening, panorama of the ways in which the intruders in our society, aided by the fruits of

modern science, have destroyed many of these traditional bastions of privacy.[4] Revelations concerning the widespread use of spike and parabolic microphones, a variety of gadgets for electronic eavesdropping, cameras equipped with modern optical devices that enable photographs to be taken at a distance and under adverse weather or light conditions, demonstrate that we do not necessarily enjoy physical privacy in our homes or offices, on the street, or while taking communion with a martini.

Now, ever increasing resort to the computer, laser technology, and microminiaturization techniques has begun to erode our informational privacy. Because the new technology makes it possible to integrate personal information from a variety of sources, solicitation lists increasingly are becoming the product of wide-ranging file investigations into the backgrounds and finances of prospective customers.[5] Personal information can be used for commercial purposes, such as generating a list of consumers with certain characteristics. *Reader's Digest* reportedly has used computer technology to produce a mailing list consisting of its subscribers' neighbors. "The approach had a kind of 'all the neighbors are doing it' quality," said one commentator. "But, more significantly, the individual was pleased that the *Reader's Digest* knew him and could relate him to others on his block."[6]

It should be evident to all that we live in an increasingly information based society. For example, ever since the federal government entered into the taxation and social welfare spheres, greater quantities of information have been sought from citizens and recorded. Moreover, in recent years access to governmental or institutional largesse has increasingly depended upon a willingness to divulge private information. As recording processes have become cheaper and more efficient, this data collection trend has intensified and been accompanied by a predilection toward centralization and collation. The effect is something akin to Parkinson's Law. As capacity for information handling has increased, there has been a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, has motivated the collection of data pertaining to a larger number of variables.

4. *See generally Hearings on Federal Data Banks and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Comm. on the Judiciary*, 91st Cong., 1st Sess. (1971); *Hearings on Commercial Credit Bureaus Before a Subcomm. of the House Comm. on Government Operations*, 90th Cong., 2d Sess. (1968); *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968); *Hearings on the Coordination and Integration of Government Statistical Programs Before the Subcomm. on Economic Statistics of the Joint Economic Comm.*, 90th Cong., 1st Sess. (1967); *Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966).

5. *See* A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 79-85 (1971).

6. N.Y. Times, July 30, 1968, at 41, col. 1.

The availability of electronic data storage and retrieval has accelerated this pattern, as is made evident by comparing the questions on a 1970 income tax form with those on a 1960 form and the significantly greater incidence of intrusive governmental, industrial, and academic questionnaires. It is now feasible to execute and evaluate these inquiries because of the availability of machine processing.

I think it is reasonable to assume that one consequence of the advent of data centers and increased computer capacity is that many governmental and private information gathering agencies will go beyond current levels of inquiry and begin to ask more complex, probing, and sensitive questions—perhaps into such subjects as associations with other people, location and activity at different points of time and space, medical history, and attitudes toward various institutions and persons.

There are additional risks lurking in the ever-increasing reliance on recorded information and third-party evaluations of a person's past performance. As information cumulates, the contents of an individual's computerized dossier appear more and more impressive, despite the "softness" of much of the data, and impart to the user a heightened sense of reliability. Coupled with the myth of computer infallibility, this will make it less likely that an independent evaluation will be made or that verification of the data will be sought. We are beginning to see more and more adherence to the file in the credit granting, insurance, educational, and employment fields.

I know a talented young lady who was unable to gain employment for some time following graduation from college because potential employers were wary of an entry in her university file that she became aware of after many painful experiences. It said: "Melinda's mother is emotionally unstable." It turned out that this comment had been made by the girl's sixth grade teacher, who was neither a psychiatrist nor a psychologist and had only met the child's mother casually. Yet this damaging entry had been preserved and had followed Melinda for 15 years without anyone questioning either its retention or its reliability. Thus, not surprisingly, many people have come to feel that their success or failure in life ultimately may turn on what other people put in their file and an unknown programmer's ability—or inability—to evaluate, process, and interrelate information. Moverover, as things now stand, a computerized file has a certain indelible quality—an adversity not to be overcome with time, absent an electronic eraser and a compassionate soul willing to use it.

The centralization of information from widely divergent sources also creates serious problems of information accuracy. I am not really speaking of the literal accuracy of the input and what is recorded in the system, although that itself becomes a more serious problem as we increase the content of dossiers and magnify the possibility of error.

Rather, I am concerned about the risks of using data out of context. Information can be entirely accurate and sufficient in one context and wholly incomplete and misleading in another. Consider the fact that computerization has made it convenient to rate an employee's efficiency and personal habits according to concise, conclusory categories such as "excellent," "fair," or "good" and that different organizations often lack common traditions of appraising or interpreting performance. Anyone not conversant with military minds and mores might be misled by a rating of "superhuman" by the United States Army, which might be equivalent to a rating of "qualified" in a more demanding organization.

The problem of contextual accuracy can be illustrated in terms of one of the most dangerous types of personal information currently maintained—the unexplained and incomplete arrest record. Is it likely that a citizen whose file contains an entry "arrested, 6/1/42; convicted felony, 1/6/43; sentenced, three years Leavenworth" will be given government employment or be accorded some of the other societal amenities of modern life? Yet our subject simply may have been a conscientious objector during the Second World War. Consider the potential effect of a computer entry "arrested, criminal trespass; sentenced, six months." Without more, how will the user know that our computerized man was simply demonstrating for equal employment in the North or desegregation in the South in the 1950's and was convicted under a statute that was overturned on appeal as an unconstitutional restraint on free speech?

In an era of great social activism on the part of the young, with counterpoint demands from others for "Law and Order," arrests are bound to increase. But many of them will be of a strikingly different character than what has been typical in the past. It is now common for hundreds of college demonstrators or black militants to be arrested in connection with one incident. Using recent experience as a guide, only a small fraction of the group will be prosecuted, and an even smaller number convicted. All of them, however, will have arrest records. Unless these records show disposition, their circulation may have an improperly prejudicial effect.

It also seems evident that the desirability of getting at a data center's enormous store of information may well offset the difficulties of gaining access to its computerized files and deciphering them, which are occasionally offered as reasons why machine readable information is inherently more secure than manually stored data. Even if we assume that the cost of securing access to computerized "dirt" is higher than the cost of dredging out the "dirt" in a more traditional form of record, the centralized quality and compactness of a computerized dossier creates an incentive to invade it because the payoff for doing so successfully may be sufficiently large that the cost per unit of computerized "dirt" actually will prove to be lower than the cost per unit

of uncomputerized "dirt."

It should not be forgotten that the risks to privacy created by data centers lie not only in abuse of the system by those who desire to injure others or who can obtain some personal advantage by doing so. There is a legitimate fear of over-centralizing individualized information and then proliferating the number of people who, by having access to it, also have the capacity to inflict damage through negligence, sloppiness, and sheer stupidity. Unthinking people are as capable of injuring others by unintentionally rendering a record inaccurate, losing it, or disseminating its contents to unauthorized people, as are people acting out of malice or for personal aggrandizement.

What then is the solution? As an initial matter, one would hope that good judgment and self-regulation on the part of the information gathering and using communities would suffice. Those who handle individualized data—whether it be in the context of financial profiles in a credit bureau, student records in a school system, medical files in a hospital, welfare lists in a governmental agency, or personnel data in a large corporation—have an obligation to guard the privacy of the human beings whose lives are reflected in those dossiers. But we must also come to grips with a basic fact of life concerning computerized information systems. The only completely effective guardian of individual privacy is the imposition of *strict* controls over the information that can be collected, stored, and disseminated. No procedural or technical safeguard is immune from human abuse or mechanical failure.

Certain types of information should not be recorded even if it is technically feasible to do so and some administrative objective would be served thereby. It has long been technically "feasible" and, from some perspectives, "desirable" to require citizens to carry and display passports when moving through the country, or to require universal fingerprinting. But the United States has not pursued these objectives because they are considered inconsistent with the philosophical fibre of our society. By the same token, absent an overpowering demonstration that the preservation of sensitive or highly personal information, such as medical and psychiatric information, or dossier-type information on those pursuing lawful political and social activities, is essential to some fundamental policy, the scrivener's hand should be stayed and the data permitted to be lost to man's memory or simply retained on a decentralized and highly confidential basis.

Another form of self-regulation that seems essential is limiting access to data. The hardware and software of any system dealing with personalized information must be designed to limit the exposure of files to a limited class of people whose access is authorized only after a careful examination of their need to know. Everyone making an inquiry into an individual file must be required to identify himself. But it must be remembered that an identification code number assigned to

each user or a magnetically coded identification card can easily be lost, stolen, or exchanged. Thus, ultimately, finger or voice prints may prove to be necessary. In addition, the system should be equipped with protector files to record the identity of inquirers and these records should be audited periodically to determine whether the system is being misused by those who have a legitimate right of access. In the same vein, it probably will be necessary to audit the programs controlling the manipulation of the files to make sure that no one has inserted a secret "door" in the protective software or modified it so that a particular password will permit access to the data by unauthorized personnel.

Because it is possible to move information into or out of a computer over substantial distances by telephone lines or microwave relays connected to terminals scattered throughout the country and even beyond, it is essential that information be protected against wiretapping and other forms of electronic eavesdropping. This risk can be minimized by coding the data or using "scramblers" to garble the information before transmission and installing complementary devices in the authorized terminals to reconstitute the signal. These procedures also will prevent "piggy-backing" or "infiltrating" the system by surreptitiously attaching a terminal to an authorized user's transmission line.

To insure the accuracy of computerized files, an individual should have access to any information in his dossier and an opportunity to challenge its accuracy. This principle has been recognized and is embodied in a new federal statute—the Fair Credit Reporting Act.[7] This enactment is the first step toward eliminating some of the abuses that result from the buying and selling of personal information by consumer reporting companies, most notably credit bureaus. It gives us a right of access to the files maintained on us by these organizations, provides a procedure for correcting any errors we might find, assures us of notice when adverse decisions are made on the basis of a consumer report, and places some restraints on the investigative reporting conducted by these firms. Although the act is full of loopholes, its basic philosophical premise, that an individual has a right to see his file, is sound and must be extended to other contexts.

Another approach might be to send a person's record to him once a year. This suggestion obviously may prove expensive, some will argue that the value of certain information will be damaged if its existence and recordation are disclosed, and it *might* produce a flow of petty squabbles that would entail costly and debilitating administrative or judicial proceedings. Nevertheless, the right of an individual to be protected against the dissemination of misinformation about him is so important that some price must be paid to effectuate it.

Finally, the information must not be allowed to petrify. Data that

7. Pub. L. No. 91-508, 84 Stat. 1127-36, 15 U.S.C. §§ 1601-77 (1970).

is shown to be inaccurate, or archaic, or of little probative value, should be deleted, reclassified, or its age brought to the attention of a user of the file.

But what if self-regulation fails? Indeed, can we afford the luxury of waiting to find out? It seems clear to me that the legal profession must become more active in finding a solution to the computer-privacy dilemma. Unfortunately, we cannot be too sanguine about the existing legal structure's ability to meet the challenge. The common law of privacy traditionally has been preoccupied with the problems raised by the mass media and has concerned itself with the commercial exploitation of a name or likeness, the offensive intrusion into an individual's personal affairs, the widespread public disclosure of private information, and the "false light" cast on individuals by media disclosures.[8]

In the constitutional law arena, recent cases seeking the expungement of files maintained by law enforcement agencies have been largely unsuccessful.[9] Despite strong arguments that the preservation of detailed information directly infringes the data subjects' right of associational privacy under the first amendment, no relief usually is given because of a judicial concern over the government's need to be able to deal with lawlessness. Furthermore, any privacy action based on constitutional rights will have to avoid the inhibiting effect of the Supreme Court's decision in *Time, Inc. v. Hill*,[10] which imposes a heavy burden of proof on the party seeking relief for an invasion of privacy.[11] The effect of that case is to give the media substantial immunity from liability for invasions of privacy in order to provide "breathing space" for freedom of expression. I think it is fair to say that this decision partially aborts the common law right of privacy's capacity for doctrinal growth.

The judicial vineyards are not completely blighted, however. The right of associational privacy is probably the most clearly developed of the constitutional protections for personal information. Thus, when the government attempts to gather data from an individual concerning his association with a group dedicated to the advancement of certain beliefs, it must show that the information sought is a subject of overriding and compelling state interest.[12] Closely related to associational privacy is another type of privacy that the courts have protected—the right to

8. *See* A. MILLER, *supra* note 5, at 173-89.

9. *See* Anderson v. Sills, 56 N.J. 210, 265 A.2d 678 (1970), *rev'g* 106 N.J. Super. 545, 256 A.2d 298 (1969). *See also* Menard v. Mitchell, 430 F.2d 486 (D.C. Cir. 1970). Judge Gesell's opinion on remand in the *Menard* case reflects a very balanced and sophisticated approach to the data bank question. Menard v. Mitchell, Civil No. 39-68 (D. D.C. June 15, 1971).

10. 385 U.S. 374, 87 S. Ct. 534 (1967).

11. *See* A. MILLER, *supra* note 5, at 190-99.

12. *See* NAACP v. Alabama, 357 U.S. 449, 78 S. Ct. 1163 (1958). *See also* Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 83 S. Ct. 889 (1963).

possess ideas and beliefs free from governmental intrusion. The leading case in this area, *Schneider v. Smith*,[13] makes it clear that espousing an unpopular idea is not a scar a person must show upon inquiry for the remainder of his life.

In a related field, a number of cases protect our physical privacy from unreasonable searches and seizures and guarantee us the "right to be let alone" in what have been described as "zones of privacy."[14] This view is exemplified by *Griswold v. Connecticut*,[15] which struck down Connecticut's attempt to regulate the use of contraceptive devices. However, a recent Supreme Court decision upholding the right of welfare authorities to terminate benefits if they are not given access to the welfare beneficiary's home under certain circumstances seems to look the other way.[16] On the plus side, mention also should be made of *Wisconsin v. Constantineau*,[17] which appears to have infused due process notions into the use of information by requiring that when a person's reputation, honor, or integrity is jeopardized by a governmental dissemination of personal information, a minimal level of procedural fairness must be satisified. But peculiarities in *Constantineau* caution us against expecting too much from it.

But these decisions simply represent the outer boundaries or constitutional limits on governmental action—they do not give us the standard for achieving the balance that is desperately needed. That will have to come from the legislature. Legislative activity in the computer-privacy field might take a number of different forms. One simple and highly desirable statutory approach would be to prohibit governmental, and perhaps even nongovernmental, organizations from collecting designated classes of sensitive data. This might be reinforced by a statutory requirement that computerized files be periodically purged of all data that has become too ancient to be trustworthy. Of course, any proposal that would have the effect of impeding the government's information practices faces an uphill battle in the political arena.

A somewhat different, and in many ways more drastic legislative approach, involves requiring computer manufacturers, users, and data networks to employ prescribed safeguards for maintaining the integrity of personal information. This can take the form of (1) imposing a

13. 390 U.S. 17, 88 S. Ct. 682 (1968).

14. *See* Stanley v. Georgia, 394 U.S. 557, 89 S. Ct. 1243 (1969); Katz v. United States, 389 U.S. 347, 350 n.5, 88 S. Ct. 507, 510-11 n.5 (1967); Berger v. New York, 388 U.S. 41, 87 S. Ct. 1873 (1967).

15. 381 U.S. 479, 85 S. Ct. 1678 (1965).

16. Wyman v. James, 400 U.S. 309, 91 S. Ct. 381 (1971). *See generally* Burt, *Forcing Protection on Children and Their Parents: The Impact of Wyman v. James*, 69 MICH. L. REV. 1259 (1971). *See also* Law Students Civil Rights Research Council, Inc. v. Wadmond, 401 U.S. 154, 91 S. Ct. 744 (1971).

17. 400 U.S. 433, 91 S. Ct. 507 (1971).

statutory duty of care on everyone connected with the data-handling process, which would encourage privacy consciousness, or of (2) enacting detailed privacy-oriented technical requirements, which would have to be followed by computer manufacturers. These would include sophisticated protective schemes involving access regulations, personnel controls, and mechanical devices that can discriminate among users and differentiate data on the basis of sensitivity that would have to be complied with by handlers of personal information.

But detailed congressional legislation is difficult to draft and the best solution may be to give over the task of regulation to an administrative agency that would act as an information ombudsman or a privacy auditor. The notion of an independent information agency is not a new one. Many of the congressional witnesses and commentators on the proposal to create a National Data Center, myself included, stressed the importance of locating control of such an organization outside the existing regulatory framework.[18] Administrative regulation would obviate the need to make highly detailed policy judgments in statutory form at what may be a premature time. It also would guarantee that the problem is placed in the hands of a watchdog group, hopefully composed of experts drawn from many fields, that could exercise continuing supervision over the data handling community.[19]

A number of Congressmen already have recognized the need for some controls and have introduced legislation to protect privacy. Unfortunately, the activity is somewhat reminiscent of Leacock's Man, who jumped on his horse and rode off in all directions at once. Bills have appeared to regulate credit bureaus, mailing list companies, the census, employee privacy, government inquiries, and psychological testing. Thus far only the Fair Credit Reporting Act, mentioned earlier, has been enacted into law. But Senator Ervin and Congressmen Gallagher and Koch have proposed broad regulation of computers and data gathering activities and we can expect continued activity in this field for some time.

When the dust ultimately settles, I hope we shall have struck the necessary balance. This probably will require give on both sides. No doubt we can coerce, wheedle, and cajole an individual into giving up part, or even all, of his informational profile. But what price would we pay for it? Alienation, distrust of the government, deceptive re-

18. *See Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968) (statement of Professor Arthur R. Miller); Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 404 (1968). *See also* Ruggles, *On the Needs and Values of Data Banks*, in *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 218-19 (1963); Zwick, *A National Data Center*, in A.B.A. Section of Individual Rights and Responsibilities, Monograph No. 1, at 32, 33 (1967).

19. This theme is developed in A. MILLER, *supra* note 5, at 228-38.

sponses, obfuscation of certain data gathering objectives (as I think may be true of the census goal of enumerating the population), numbing of privacy values, and an atmosphere of suspicion. Instead of the stick, perhaps we should rely on the carrot. Governmental and private planners must refine their information handling techniques, reduce the burden on the individual, and assure us accuracy of the files and security against improper dissemination. If this is done, perhaps we will feel less apprehensive about yielding a little of ourselves. Few aspects of life, even in a free society, can survive as absolutes—and that includes privacy.

If some of my remarks seem slightly alarmist in tone, it is because I feel it is necessary to counteract the syndrome referred to by the poet e.e. cummings, when he wrote "progress is a comfortable disease."[20] We must overcome the all-too-often complacent attitude of citizens toward the management of our affairs by what frequently are astigmatic administrators in both government and the private sector. The very real benefits conferred by information technology may opiate our awareness of the price that may be exacted in terms of personal freedom. It thus seems desirable to sound the klaxon to arouse a greater awareness of the possibility that the computer is precipitating a realignment in the patterns of societal power and is becoming an increasingly important decision-making tool in practically all of our significant governmental and nongovernmental institutions. As society becomes more and more information oriented, the central issue that emerges to challenge us is how to contain the excesses and channel the benefits of this new form of power.

If the concept of personal privacy is fundamental to our tradition of individual autonomy, and if its preservation is deemed desirable, then I feel that the expenditure of some verbal horsepower on its behalf is justified. Unless we overcome inertia, there will be no one to blame but ourselves if some day we discover that the mantle of policymaking is being worn by those specially trained technicians who have found the time to master the machine and are using it for their own purposes. To paraphrase the French sociologist, Jacques Ellul, that it is to be a dictatorship of dossiers and data banks rather than of hobnailed boots will not make it any less a dictatorship.[21]

20. e.e. cummings, 100 SELECTED POEMS 89 (paperback ed. 1959).
21. J. ELLUL, THE TECHNOLOGICAL SOCIETY 434 (paperback ed. 1964).

[EXCERPTS FROM THE UNIVERSITY OF ILLINOIS LAW FORUM, VOL. 1971, NO. 2]

Copyright 1972 by the Board of Trustees of the University of Illinois

PRIVACY AND THE POOR†

*Michael Harrington**

THE TOPIC I will discuss was dramatized recently when President Nixon addressed the White House Conference on Children. He told of how his daughter Tricia had visited a school and had been terribly upset because at lunch time the children who brought their own lunches were permitted to stay in the classrom and eat, but the children who got free lunches were required to eat in an auditorium. Mr. Nixon stated, "We have got to find ways of ending . . . [this] stigmatizing by separation of the welfare children as welfare children."[1] For once, I agree completely with the President of the United States. Poor people have a right to dignity; their misery must not be aggravated by discriminatory treatment.

Before I get to the subject of poverty and privacy, however, I should like to put into context the importance of privacy to our society as a whole. As Kenneth Boulding put it in a telling metaphor, the growth of population in the world and the strain on our resources is now such that we must consider ourselves as riding space ship Earth.[2] We are going to have to recycle more and more of life's processes; we are going to have to organize life much more carefully if it is to sustain everyone. So the process of survival is going to menace the privacy of us all. In that sense, I think that the issue of privacy—in particular, one's ability to be free from bureaucratic intrusions—is one of the basic issues of our times.

This morning I shall look at invasions of privacy particularly from the point of view of the poor—first, as a system of legal discrimination against the poor; second, I shall touch on extralegal discrimination which, I think, affects the privacy of the poor to an even greater extent than does legal discrimination. Finally, I shall draw some conclusions about the nature of the law in relation to poverty and privacy and the direction which it ought to take.

Through a system of legal discrimination, the government has in-

† *These remarks were originally delivered as a lecture in the Privacy and the Law Series at the University of Illinois College of Law, December 15, 1970.*

* *A.B. 1947, Holy Cross College; M.A. 1949, University of Chicago.*

Mr. Harrington, who attended Yale Law School for a year, was George A. Miller Visiting Professor of Law at the College of Law during the fall 1970-71 semester.

1. N.Y. Times, Dec. 14, 1970, at 19, col. 1.
2. K. BOULDING, BEYOND ECONOMICS 285 (1968).

creasingly encroached upon the privacy of everyone. Since most people in the labor market earn their income from jobs, their privacy usually has not been invaded. More and more, however, invasions of privacy are appearing even in the labor market. For example, black lists, which developed in the 1950's for all kinds of government jobs, are now used in government-related jobs to aid in the employment, or more appropriately the unemployment, of stevedores and seamen. They are also used in the movie and television industry to eliminate so-called undesirables on the basis of past activities. Recently, the House Internal Security Committee, the successor to the House Un-American Activities Committee, compiled a new list of allegedly radical college campus speakers and how much money each had received.[3] The list is a not too subtle hint to college administrators not to engage these people as speakers in the future.

In addition to government probes into personal privacy, the enormous growth of credit as an institution has given rise to a huge private bureaucracy which now checks on people. This development struck home fortuitously several years ago when, due to a small misunderstanding with American Express, my credit card was cancelled. I had called Avis to rent a station wagon and was informed by a young lady that Avis did not rent station wagons to people who had only money with no credit. In short, the denial of my credit privileges for a while meant that I could not rent an automobile. In response to my entreaties the young lady acknowledged that a quick credit check could be run to establish my credit. When she learned that I had no employer, however, she replied that in that case it would be rather difficult to run a quick credit check. But Avis does try harder. When I stated that I was a writer, that I had just had a book published, and that my picture was on the back of the book, she conceded that that would establish me as a man of means in the community. So I took a copy of *Toward a Democratic Left* to the Avis office for my quick credit check, and I got the automobile. My point in telling this anecdote is that in terms of credit, one's privacy—middle class privacy—is being subverted by private and largely unregulated bureaucracies.

The poor and their privacy are related in a somewhat different fashion. Many poor people get their incomes from welfare, and, as a price of getting welfare, they make an enormous surrender of their right to privacy. In a sense they have to pay for welfare. Let me make it clear at the outset, however, that not all poor people are on welfare. Most poor people are not; so when I talk about the problems of poverty, privacy, and welfare, I am talking only about one-third of the poor.[4]

3. Further publication of the list has been enjoined. Hentoff v. Ichord, 318 F. Supp. 1175 (D.D.C. 1970).

4. Armstrong, *The Looming Money Revolution Down South*, FORTUNE, June 1970, at 66, 152.

Indeed, I suggest that the invasion of privacy which accompanies welfare is designed to keep these people off welfare. The welfare system hounds the poor in such a way that those who are unwilling to surrender their privacy will not apply for welfare.

One of the excuses for forcing those on welfare to surrender their privacy lies in the widespread American assumption that people on welfare are lazy cheats. There is, therefore, no general revulsion over welfare applicants being investigated carefully and their statements thoroughly checked out. Recently, however, an interesting experiment has been carried out in a series of pilot programs. We have taken poor people at their word. Rather than conducting meticulous investigations into their alleged impoverishment, we have asked them simply to state in their welfare applications what they have and what their situation is. We have told them that their statements will be believed. In these experiments, a certain percentage of applications has been spot checked to determine the extent of cheating. We have discovered that poor people do cheat somewhat but not very much. Indeed, the percentage of misstatements on welfare applications is less than that of upper and middle income people when they file their tax returns. These people, however, are outraged to hear of poor people cheating on welfare, although their own federal income tax returns become a work of high art and imagination. So, one source reports, the federal government has decided on pragmatic grounds to stop this unnecessary invasion of privacy. The Department of Health, Education and Welfare will now require welfare departments to adopt the procedure of trusting the poor and not checking on every statement in deciding who is qualified for benefits.[5]

A second example of the invasion of the privacy and the dignity of the poor is the requirement that in many situations poor persons reveal and give up the possibility of future income in order to qualify for welfare.[6] If a welfare applicant has any possible asset, he may have to deed it over to the state. For instance, as a price of getting welfare now, he may have to give up a pending lawsuit that could bring him some money in the future and make him independent again. He has to show himself to be totally destitute.

Third, there is an invasion of privacy which anybody can observe in the supermarket. When a person who has food stamps goes into a checkout line, he finds a sign stating that he must declare himself. So he has to stand there and raise his hand and say, "I am poor, because I've got food stamps." Furthermore, that sign tells him that there are certain foods he cannot buy with food stamps; that his use of the

5. St. Louis Post Dispatch, Dec. 13, 1970, at 1B, col. 4.

6. *See, e.g.*, ILL. REV. STAT. ch. 23 § 3-10 (1969) (lien on real property of welfare recipients).

stamps is circumscribed.

But perhaps the most ruthless invasion of privacy is the famous man-in-the house rule, which states that a mother cannot receive aid for dependent children if there is a man in the house. In a good many states, the rule held true even if the man was the woman's husband. These are the states which do not participate in the Aid for the Dependent Children of the Unemployed program; therefore, a jobless husband has to leave his home in order to feed his family. Consequently, a clear correlation between unemployment and marriage breakups exists in areas such as Appalachia. The man-in-the house rule has recently been held unconstitutional in many situations by the courts,[7] and it appears to be on the way out. At this moment in Congress, however, the Dixiecrat senators are trying to write the rule into the Family Assistance Plan,[8] even though the Supreme Court has held in a very important case that aid for dependent children is aid to children which cannot be withheld because of the alleged sins of the mother.[9] In spite of this clear holding, those senators refuse to abandon their backing of the rule. As you know, the effect of the man-in-the house rule is to allow welfare investigators to make sneak attacks on houses to determine whether evidence of men living therein exists. These attacks become, in the terms of privacy, outrageous attempts to police the morals of the poor. Only poor people are required to be moral in this society in order to get their money. The rest of us may be sinners, yet we demand a higher standard of morality on the part of the poor than we do of ourselves.

Why is this? Why are there so many rules and regulations permitting invasion of privacy of the poor? Why so many questionnaires? Why the requirement of complete destitution and the supermarket declarations of poverty? Why must the poor be subject to raid by welfare officials to see if there is a man around? I would suggest one reason is that ours is a very moralistic society, which feels that poor people should be deserving before they should receive their handout. Lester Maddox put it most bluntly when he said, "[T]hey should be made to feel like the bums that they are."[10] Unfortunately, that point of view is shared by a good many people in this society.

The second and I suspect more important reason is that the invasions of privacy which accompany welfare payments tend to keep people off welfare. Often poor people do not apply for welfare because they

7. *See, e.g.*, Ojeda v. Hackney, 319 F. Supp. 149 (N.D. Tex. 1970).

8. H.R. 16311, 91st Cong., 2d Sess. (1970). The Senate defeated the Family Assistance Plan two weeks after this lecture was delivered, N.Y. Times, Dec. 29, 1970, at 1, col. 1. The bill has been reintroduced this session. H.R. 1, 92d Cong., 1st Sess. (1971).

9. King v. Smith, 392 U.S. 309, 88 S. Ct. 2128 (1968).

10. Armstrong, *supra* note 4, at 68.

do not know how to cope with these invasions. Indeed, the invasions are designed to discourage them. The welfare system also makes poor people dependent on the whims of administrators, because welfare is not a right; it can be taken away. There is resentment over this dependency, and it keeps people off the welfare rolls. I am convinced that one of the main causes of the recent increase in welfare rolls in cities like New York[11] has been that organizations like the National Welfare Rights Organization have elevated people for the first time to feel that they have a *right* to welfare, that they do not have to go hat in hand submitting passively to these invasions of privacy. These organizations have allowed the poor to preserve their humanity and have taught them to fight back. As a result, more people are taking advantage of the welfare rights they have always had.

Finally, I think that these invasions of privacy in the South are a means of controlling the labor market and controlling black people; that is, when welfare payments are dependent upon conduct and when administrative discretion to pay or not to pay benefits is broad, there exists a potentially effective apparatus for keeping people in their "place." There is guaranteed a supply of cheap, docile labor if, for instance, one can be removed from welfare for registering to vote. Paradoxically, however, it is the South that would gain the most if the Family Assistance Plan passed.[12] The white southern poor would gain even more than the black southern poor because there are more poor whites in the South than poor blacks. Moreover, southern businessmen would gain substantial income, since a welfare family in Mississippi which now gets $39 a month, for example, would get about five times that amount.[13] Yet most Dixiecrats are against the Family Assistance Plan. If the Family Assistance Plan goes through, 35 per cent of the people of Mississippi, 25 per cent of those in Louisiana, and 22 per cent of all Georgia residents would receive some federal money.[14] Yet, the Senators from these three states are fighting against the program which would provide benefits for so many of their own people.[15]

Why is there this opposition? I suggest that they are fighting the plan because they fear what it will do to the labor market. As Representative Landrum of Georgia put it, "There's not going to be anybody left to roll these wheelbarrows and press these shirts."[16] In terms of the availability of cheap labor, his fears are probably justified. A woman

11. N.Y. Times, Dec. 13, 1970, at 1, col. 6.
12. *See Hearings on H.R. 16311 Before the House Comm. on Rules*, 91st Cong., 2d Sess. 114 (1970).
13. Herman, *Welfare Reform: The Southern View*, Wall St. J., Dec. 15, 1970, at 22, col. 4.
14. *Id.*
15. *Id.*; N.Y. Times, Nov. 25, 1970, at 75, col. 1.
16. Armstrong, *supra* note 4, at 68.

would have to be crazy to wash and press Landrum's shirts if her wage for doing so is less than what is available to her through welfare. I think the Dixiecrats are terrified of the destruction of their cheap labor supply, and they are terrified above all that black people would no longer be so dependent on the whim of local authorities.

An article in the *Wall Street Journal* makes this point with some telling quotations. One was from a Texas real estate investor, who, talking in horrified tones about the consequences of passing the Family Assistance Plan, said: "These ethnic groups, and the Negroes, they don't want to say 'Yes sir,' they want to sit down and have coffee with you."[17] And he then said, "You give all these people more money and you'll get more of them voting, which means there will be more left wingers running for office and winning because of the bloc vote. And Lord knows, we've got enough left wingers as it is."[18] I think that is a clear statement why the racist South resists a plan which would help all of the poor.

In conclusion, there now exists a system of legal discrimination against the poor which can and should be eliminated. We should at the outset abandon the nonfunctional invasions of privacy now in the welfare system. We should accept the word of the poor and discard the man-in-the house rule. Most dramatically, we should give people money and not stamps to buy food. Ideally, the poor should receive their income as of right. Benefits should not be conditioned on moral righteousness and bureaucratic approval. As it now exists, poverty is a malady which the law will help to remedy in exchange for the privacy of the impoverished. I think this is scandalous.

In addition to legal invasions of privacy, the poor are constantly exposed to extralegal invasions. These I consider even more important than the legal invasions. Even if all of the laws that invade the privacy of the poor are changed and the welfare system is designed precisely as I idealize it, the poor would still have much less privacy than anyone else. The reason is that, unlike anyone else, the poor are jammed together in large numbers in miserable buildings. Indeed, one could almost define urban poverty in terms of absence of privacy. It is a fact of life that in such housing privacy cannot exist. The consequences are far-reaching. Researchers have discovered, for example, that this lack of privacy has a profound impact on the mental health of the poor. Although it is generally known that the middle and upper middle classes in suburbia have problems of alcoholism and infidelity and some have even greater problems of neurosis and psychosis, it is often thought that the poor in the ghettos and in the backwoods are noble savages, who, although physically deprived, have retained a kind of animal vitality.

17. Herman, *supra* note 13, at 22, col. 6.
18. *Id.*

Recent studies of the incident of neurosis and psychosis, however, show that the poor have qualitatively more neurosis and psychosis than any other social class. Psychologists cite lack of privacy as one reason for this result. In the Freudian model of the personality, basically a middle class model, it is the mother figure, father figure, and siblings which are the decisive personalities in the development of a human personality. But research suggests that under conditions of poverty in which everybody is jammed together, the developing personality also becomes aware of these personalities infringing on its life. Noisy conditions with people concentrated in small quarters can scar the personality. Therefor, I suggest that the simple lack of physical privacy in a slum may be a factor in causing nervous breakdowns and neurotic and psychotic character traits.

Lack of privacy also impinges on one's sexuality. The fact that poor families often must live in single rooms not only inhibits normal adult relations but makes it commonplace for small children to become immediately acquainted with sex and frequently with its more sordid aspects. Thus, lack of privacy affects both the mental health of the poor and that intimate and important part of human existence that sexuality occupies. Indeed, the extraordinary thing about the poor is the degree to which they are able to resist the pressures they face and find within themselves the strength to lead stable and, in some cases, productive and creative lives.

The most critical aspect of the poverty and privacy crises, then, is the housing problem, and as long as America permits this problem to go unsolved, it is kidding itself that it cares about poverty, privacy, or anything else. Some years ago in Washington, D.C., I saw an excellent example of what can be done to alleviate poverty and invasions of privacy which relate to housing inadequacies. Someone challenged the sincerity of a couple of young men involved in Americans for Democratic Action (ADA) by declaring that ADA was only a parlor exercise in progressivism and that they really should do something. So these men purchased some buildings in a black slum in Washington in which people had been living one family to a room and moved three quarters of the people to other apartments. The one quarter of the families that remained worked hard to repair and renovate the houses. Each family occupied a floor instead of one room, and each had its own bathroom and kitchen where previously each of these facilities had serviced the entire building. The result was that these houses, architecturally old and rich, became just as attractive as those homes which Georgetown now provides for the well-to-do. The primary reason why the black slum is less beautiful than Georgetown is that there are too many people in it. Obviously, the solution to that and related problems is to reduce the density of people and provide decent housing.

In saying this, I am trying to avoid the trap into which some fall in assuming that absolute numbers are a social problem. Our problem in this country is not yet the number of people we have, but how we organize the conditions of their lives. A population problem exists—but if we had imaginatively tried to deal with it by building new cities and towns it would be much less of a problem than it is today. Instead we have funneled masses of poor into large city ghettos. Even the repeal of anti-privacy laws would give the poor little privacy, because most of them would necessarily continue to carry out some of the most intimate aspects of their lives in the semi-public conditions caused by overcrowding and poor housing. This lack of privacy affects their emotional stability and sexual life as well as most other intimate aspects of their family life. In short, it is impossible to romanticize slums and ghettos. Although some families of extraordinary strength have emerged from these conditions, the majority has no chance. Therefore, priority must be given to the creation of decent housing for everyone in the United States if the problems associated with poverty and lack of privacy are to be combatted.

Finally, let me generalize about what the law means and has meant. Traditionally in this country, although not only in this country, the law has been thought of in negative terms and privacy in particular has been thought of in negative terms. The responsibility of the law in respect to privacy has traditionally been to leave people alone, to interfere minimally with their lives. This philosophical attitude stems from philosophers like Hobbes and Kant who believed that each individual in society pursued his own personal goal and that the function of the law was simply to stop people from colliding with one another. Their image of society was basically an unsocial one.

I have another image of society which differs markedly from the Hobbsian or Kantian idea of the unsocial society. My image is of a society in which people, rather than simply not hurting each other, act positively to help one another. Conceptually, I see the law not as a negative force or as a restraint but as a positive, creative force. In the areas of privacy and poverty, however, the law can aid by functioning, in philosophical terms, both negatively and positively.

First, from a negative point of view, there should be a presumption that the privacy of the poor is not to be violated; that is, we must presume that poor people are no different from other people in the society. They must not be required to surrender any of their rights in order to get assistance from the state when assistance is needed. We must allow that presumption to be defeated only when it is shown that investigating a poor person has a function which will actually help that person's welfare. The invasions of privacy which we now tolerate cannot be justified on the grounds that poor mothers should be more faithful than middle class mothers or that poor men and women should abstain from drink-

ing and so forth and so on. We must abandon our present attitude towards welfare and instead presume a right to privacy. Lawyers must present and courts apply that presumption.

Second, still from the negative point of view, laws must be enacted to control bureaucracies in the area of welfare as well as in many other areas of American life. I suggested the appropriate weapon some time ago, and I reemphasize it now. What we need in this society is a National Bureaucratic Relations Act similar to the National Labor Relations Act. Prior to the National Labor Relations Act, we assumed that conflicts between labor and management were private and within contractual confines. A different outlook emerged in the 1930's, brought on primarily by the struggle of millions of working people. This country realized that a social structure had to be established in which struggles between management and labor could take place. Society asserted its ultimate power and laid down the rules of the game. I suggest now that for the poor especially the problem of bureaucracy is increasing. We need legislation which would establish the rights of citizens vis-á-vis the bureaucrats. For example, I imagine one aspect of the legislation would be to require every bureaucracy to establish an independent review board similar to the independent review board of the United Automobile Workers' Union. A group of people independent of the bureaucracy would then review all complaints against that bureaucracy. A charge of police brutality, for instance, would be investigated by an independent civilian board and not by the police, who have a certain self interest in clearing themselves. All welfare institutions should also be overseen by an independent review board, so that grievances can be reviewed by someone outside of the system. A major problem that the poor often face with the police, the school system, or the welfare system is that their complaints go only to the associates of those against whom their complaints are directed. Therefore, if we are to protect the poor from bureaucratic intrusions we must have a Bureaucratic Relations Act complete with independent review boards.

A third area in which the law can be helpful in a negative sense is by removing the constraints occasioned by zoning. One of the reasons why poor people are concentrated as they are is that so many of our cities have the famous white noose around the black central cities. Zoning restrictions keep people jammed together, making it impossible to break out into the privacy which suburbia offers. To challenge these zoning restrictions in order to provide access to privacy for poor people, not only must existing legal principles be used but new legislation must be sought.

Let me now turn to positive ways in which we can act to get bureaucrats and laws off the backs of the poor. I think only in the sphere of positive, creative action will the issue of privacy for the poor be set-

tled. We must take positive action to eliminate nonfunctional invasions of privacy. Moreover, unless we solve the housing problem, we will be unable to give the poor privacy no matter what else we do. To solve the housing problem adequately will require planned investments of billions of dollars. On a broader plane, we are going to have to plan the use of many other things, such as beaches. In the New York City area every community which has ocean beaches is beginning to put restrictions on the use of those beaches. Beachfront communities do not want city folks coming out and making the beaches less private. The motivation behind the restrictions may not be consciously racist. Nevertheless, these restrictions, just as zoning restrictions, particularly strike out against Blacks, Puerto Ricans, and other minorities. We must work to plan the use of beaches and other limited facilities for everyone.

Paradoxically, if there is to be more privacy for everyone in our society, we are going to have to rely increasingly on public planning. This is paradoxical because it would seem that to increase public planning would remove more from the sphere of private influence and place it into the area of public decision. I think, however, that is the only way to deal with these problems. I also think in terms of resolving the more important issues associated with privacy and poverty that there will have to be a political struggle. A legal struggle will not be enough. I cite as support for my theory the recent events involving the man-in-the house rule. The Supreme Court in striking down the man-in-the house rule, properly stated that the Social Security Act provided monies for children not for mothers, and that it was unlawful to take money away from kids on the basis of what their mothers might have done. But no sooner had we begun to move towards a rational policy by abandoning the outrageous invasions of privacy inspired by the man-in-the house rule than the reactionaries in Congress counterattacked through the proposed Family Assistance Plan. They have set as their price of approval of a minimum income for poor people in the United States the reestablishment of the man-in-the house rule.

So, if I may summarize briefly, I suggest to you first in terms of law that the poor legally have less privacy than any of us—particularly those poor who are on welfare and who are required for nonfunctional reasons to surrender a good deal of their privacy to investigators who police their morality. Second, even if all legal discrimination were eliminated and legal invasions of privacy stopped, the economic and social conditions under which most of the poor live would still allow them little privacy. The dense concentration of the impoverished has affected their mental health, sexuality, family life, and just about every other aspect of their existence. Third, I propose that we should deal with these problems by taking positive action to create an environment in which the possibilities for privacy for poor people are enhanced. This change would mean getting poor people out of the urban concen-

tration camps in which they have been locked by so many economic, social, and legal policies. It would mean getting them out where they too could enjoy space, air, and privacy. This change has ultimately to be made politically. To make a summary point on this area and on the whole subject of poverty, I am really not saying that we should treat the poor better than anyone else; all I am saying—and it is a radical thing to say—is that we should treat the poor not as people who have a special right to privacy but only as people who have a moral, political, legal, and social right to as much privacy as the rest of us in this society enjoy.

VOL. 22 JOURNAL OF PUBLIC LAW (1973)

THE FAIR CREDIT REPORTING ACT: A LEGISLATIVE OVERVIEW

By
Robert M. McNamara, Jr.*

"If your name is not in the records of at least one credit bureau, it doesn't mean you don't rate. What it means is that you are either twenty-one or dead."

H. BLACK, BUY NOW, PAY LATER 37 (1961)

"We have become the greatest data-generating society in human history."

A. WESTIN, PRIVACY AND FREEDOM 159 (1967)

IN ONE OF ITS VARIOUS FORMS, CREDIT is probably one of the oldest constants of any economic system. It exists today in as widely divergent social groups as the food-gathering societies of the South Pacific, the rural co-ops in Africa, and the World Bank. In some areas, such as the United States, it has almost completely replaced money as a form of exchange. As one author has said, "Ours is a credit economy."[1] Many causes have contributed to this situation: the auto loan, the installment contract, the revolving charge, and, of course, the credit card. Various reasons for this phenomenon could be given ranging from simple convenience to conspicuous consumption to socio-economic evolution. The fact is, however, that the credit system is with us and all indications are that it has become a permanent fixture in the average American's daily life.

---

*B.A. Mount Carmel College; A.B. John Carroll University; J.D. Georgetown University. The author would like to acknowledge his appreciation to Ms. Judith F. Dobkin for her assistance in the final preparation of this article.

[1]W. KAYE & ASSOCIATES, CONSUMER CREDIT AND THE LOW-INCOME CONSUMER (Preliminary Report) i (1969). Since 1950, the outstanding consumer credit has risen from $21 billion to $113 billion in 1968. *Id.* at 3. In 1967 consumer credit in the United States was $95 billion, exclusive of home mortgages. It has been estimated that 60 percent of the average individual's income now goes to pay off credit obligations. *Hearings on Commercial Credit Bureaus Before a Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 90th Cong., 2d Sess. 5 (1968) [hereinafter cited as *Hearings on Commercial Credit Bureaus*] (Statement of Dr. Alan F. Westin, Professor, Public Law & Government, Columbia University). Consumer credit is extended at the rate of $8 billion per month, TIME, Dec. 20, 1968, at 79, and was equal to 19 percent of disposable personal income in 1969. U.S. BUREAU OF STATISTICS, STATISTICAL ABSTRACTS OF THE UNITED STATES 317 (1969). The growth of consumer credit since 1945 has been at the rate of four and one half times the growth rate of our national economy. 1969 U.S. CODE CONG. & AD. NEWS 1965-55. Between 75 and 81 percent of the population use credit for purchases. D. CAPLOVITZ, THE POOR PAY MORE 100-01 (1963).

As the use of credit grew and became an ordinary method of transacting business, it also became more risky for businesses, and, consequently, certain safeguards were necessary to protect those who were extending credit to their customers. Originally, merchants exchanged information regarding the credit reliability of their customers. When there was a lack of information on a particular person, an agent was sent to collect sufficient information to determine his credit-worthiness.[2] The agents gradually evolved into agencies which functioned as independent contractors.[3] The growth of these mercantile or credit agencies paralleled the increasing use of credit in everyday transactions. Today these credit agencies are, to a certain extent, essential to the maintenance of a credit economy.[4] They are also big business.

These credit agencies gather information concerning the credit-worthiness of individuals and corporations engaged in trade or commerce and pass it on to their subscribers so that they may conduct business with a minimum of risk.[6] The function performed by credit agencies is vital if lenders and

---

[2]State v. Morgan, 2 S.D. 32, 52-54 (1891), outlines the general evolution and history of credit bureaus.

[3]*See* Note, *The Mercantile Agency and Conditional Privilege in Defamation*, 11 S.C.L.Q. 256, 261 (1959).

[4]A credit bureau is any person, firm, partnership, corporation, organization, association, or any other legal entity engaged in gathering, recording and disseminating favorable as well as unfavorable information relative to the credit-worthiness, financial responsibility, paying habits, and character of individuals, firms, corporations, or any other legal entity being considered for credit extension, so that a prospective creditor may be able to make a sound decision in the extension of credit. *Hearings on Commercial Credit Bureaus*, *supra* note 1, at 104 (Statement of John J. Spafford, Executive Vice-President, Associated Credit Bureaus of America, *citing* the definition embodied in the Federal Trade Commission industry guides).

[5]The Associated Credit Bureaus of America has over 2,200 member bureaus, servicing 400,000 "credit grantors in 36,000 communities across the nation and in many foreign countries. Its members maintain credit files on more than 110 million individuals, and in 1967 they issued 97.1 million reports." *Hearings on Commercial Credit Bureaus*, *supra* note 1, at 5 (Statement of Dr. Alan F. Westin). In 1968, the Wall Street Journal discussed the future of these files:

> Eventually any of Associated Credit Bureau's 110 million files will be available to local bureaus at the touch of a button. A.C.B., working with International Business Machines Corp., and the Dallas and Houston credit bureaus, is designing a computerized system that it expects to become nationwide in time. A central switching system will connect computers at all local bureaus.

Wall Street Journal, Feb. 5, 1968, at 1, col. 6, and at 12, col. 1. Credit Data Corporation, a California-based operation, already has approximately 20 million individuals in its computerized files and can retrieve information on an individual in approximately two minutes. *Hearings on Commercial Credit Bureaus*, *supra* note 1, at 68 (Statement of H.C. Jordan, President, Credit Data Corp.). This system has added to it approximately 50,000 new files a week. *Id.* at 69. Asked how long it would be before every American's name would be listed with Credit Data Corp., Dr. Jordan replied, "[W]e regard it as approximately a five-year job." *Id.*

[6]*See* Mitchell v. Bradstreet Co., 116 Mo. 226, 231, 22 S.W. 358 (1893).

merchants are to be protected and the free flow of credit maintained.[7] Those who are extending credit have a recognized right to protect themselves from poor credit risks which, if allowed to go unchecked, would eventually destroy the credit system. Credit agencies facilitate commercial transactions by providing businessmen with easily accessible information concerning the credit and financial standing of others with whom they may wish to deal. The necessity of such information cannot be questioned. Nor can it be questioned that the agencies, in supplying the information, are fulfilling a legitimate business need.[8] The problem surfaces when the information furnished contains false or libelous or incomplete statements. On the basis of the service performed and the benefits conferred, both of which reflect upon the basic health of the credit economy, credit agencies have been given a special form of protection when action for defamation has been brought against them. This protection is referred to as a conditional or qualified privilege.

The Law of Qualified Privilege

The concept of privilege centers around the desirability of protecting the particular interest involved, *i.e.*, the interest of the recipient of the information in protecting himself from poor credit risks.[9] Yet, what is actually determined by allowing such protection is the importance of the service in relation to the importance of an individual's reputation. If the privilege is to be granted, the social value of the interest sought to be protected by the privilege must have greater importance than the interest of the defamed person in obtaining compensation for damage to his reputation.[10] In short, it is a matter of public policy.[11]

The effect of such a policy is to grant immunity on the basis of social necessity or convenience,[12] whereas one not granted immunity is held strictly liable regardless of circumstances or excuse.[13] The privilege, however, is not absolute as in the cases of legislative or judicial immunity.[14] It is, as its name implies, subject to certain conditions. The general rule is that information must be furnished in good faith to a subscriber having a legitimate interest in the information.[15] The privilege does not make the matter any less defam-

---

[7]Note, *Credit Investigations and the Right to Privacy: Quest for A Remedy*, 57 GEO. L.J. 509, 532 (1969).

[8]Petition of Retailers Commercial Agency, Inc., 342 Mass. 515, 174 N.E.2d 376, 379 (1961).

[9]*See* Note, *supra* note 3, at 261.

[10]*Id.* at 258. *See* W. PROSSER, HANDBOOK OF THE LAW OF TORTS 796 (3d ed. 1964).

[11]*See* 3 RESTATEMENT OF TORTS 340 (1938) (Scope Note).

[12]*See* Note, *Privileged Defamation*, 22 VA. L. REV. 642 (1936).

[13]*See* Note, *supra* note 3, at 257; W. PROSSER, *supra* note 10, at 791.

[14]W. PROSSER, *supra* note 10, at 796-805.

[15]*See* Erber & Stickler v. R.G. Dun & Co., 12 F. 526 (C.C. Ark. 1882); Sunderlin v.

atory; it merely refutes the legal inference of a presumption of malice and shifts the burden of pleading and proving its actual existence onto the plaintiff.[16] Some courts have discarded the test of malice and supplied in its place wanton and reckless disregard[17] or the lack of reasonable or probable grounds.[18] Although most courts have explicitly rejected negligence as a sufficient abuse,[19] a few have accepted the absence of due care as sufficient reason to remove the privilege.[20]

There are other abuses of the privilege which can result in its loss. General publication of the information to those not having an interest in it has been

---

Bradstreet, 46 N.Y. 188 (1871); Ormsby v. Douglas, 37 N.Y. 477 (1868); Bradstreet v. Gill, 72 Tex. 115, 9 S.W. 753 (1888).

Prior to the effective date of the Fair Credit Reporting Act, a husband and wife, in separate suits, sought to recover damages from a credit company, alleging libel in both cases and invasion of privacy in the husband's suit. On the wife's appeal, the court upheld the summary judgment for the credit company based on qualified privilege. Wilson v. Retail Credit Co., 438 F.2d 1043 (5th Cir. 1971). On the husband's appeal, summary judgment in favor of the credit company was also upheld on the ground of qualified privilege. Wilson v. Retail Credit Co., 457 F.2d 1406 (5th Cir. 1972).

[16]*See* Stice v. Beacon Newspaper Corp., 185 Kan. 61, 340 P.2d 396 (1959). The concept of malice, however, is difficult to define. *See* Hallen, *Character of Belief Necessary for the Conditional Privilege in Defamation*, 25 ILL. L. REV. 865, 865-66 (1931). Moreover malice is rarely present, and is difficult to prove when it is. *See* Note, *supra* note 3, at 263; Note, *supra* note 7, at 516. Perhaps for this reason, Professor Prosser had characterized it as a "meaningless and quite unsatisfactory term," and suggests that it be discarded. W. PROSSER, *supra* note 10, at 882.

The effect of the term as it is used and applied by the courts is, as two writers have pointed out: "a protection . . . that borders on absolute immunity from liability in defamation." Note, *supra* note 3, at 263; Note, *supra* note 7, at 516.

[17]A.B.C. Needlecraft Co. v. Dun & Bradstreet, Inc., 245 F.2d 775 (2d Cir. 1957); H.E. Crawford Co. v. Dun & Bradstreet, Inc., 241 F.2d 387 (4th Cir. 1957); Mil-Hall Textile Co. v. Dun & Bradstreet, Inc., 160 F. Supp. 778 (S.D.N.Y. 1958); Dun & Bradstreet, Inc. v. Robinson, 233 Ark. 168, 345 S.W.2d 34 (1961); Petition of Retailers Commercial Agency, 342 Mass. 515, 174 N.E.2d 376 (1961).

[18]*See* Douglas v. Daisley, 114 F. 628 (1st Cir. 1902); Stationers Corp. v. Dun & Bradstreet, Inc., 62 Cal. 2d 412, 398 P.2d 785, 42 Cal. Rptr. 449 (1965); Cullum v. Dun & Bradstreet, Inc., 228 S.C. 384, 90 S.E.2d 370 (1955). *But see* H.E. Crawford Co. v. Dun & Bradstreet, Inc., 241 F.2d 387 (4th Cir. 1957); Pecue v. West, 233 N.Y. 316, 135 N.E. 515 (1922).

[19]*See* A.B.C. Needlecraft Co. v. Dun & Bradstreet, Inc., 245 F.2d 775 (2d Cir. 1957); Mil-Hall Textile Co. v. Dun & Bradstreet, Inc., 160 F. Supp. 778 (S.D.N.Y. 1958); Stationers Corp. v. Dun & Bradstreet, Inc., 62 Cal. 2d 412, 398 P.2d 785, 42 Cal. Rptr. 449 (1965); Petition of Retailers Commercial Agency, 342 Mass. 515, 174 N.E.2d 376 (1961); Pollasky v. Minchener, 81 Mich. 280, 46 N.W. 5 (1890). *But see* Corrigan v. Bobbs Merrill Co., 228 N.Y. 58, 126 N.E. 260 (1920); Crew v. Bradstreet Co., 134 Pa. 161, 19 A. 500 (1890).

[20]*See* Altoona Clay Prods., Inc. v. Dun & Bradstreet, Inc., 367 F.2d 625 (3d Cir. 1966); Serino v. Dun & Bradstreet, Inc., 267 F. Supp. 396 (D.S.C. 1967); Dun & Bradstreet, Inc. v. Robinson, 233 Ark. 168, 345 S.W.2d 34 (1961); Berry v. Moench, 8 Utah 2d 191, 131 P.2d 814 (1958).

held by the courts to remove the credit agency from the scope of protection.[21] In a very few cases, the privilege itself has been completely denied generally because of the profit motive involved in supplying the information.[22] These courts reasoned that the pecuniary element cast an otherwise protected interest into a different light. When weighing the interests involved in light of the profit characteristic, the courts have held the agencies to a standard of care, and the individual's reputation has been considered of greater importance than the benefit conferred upon the businessmen by the agencies. Unfortunately, these cases stand out as unique in their concern for the individual as well as for the potential harm that could be caused by agencies given the protection and immunity afforded by the privilege.

Congressional Attention—The National Data Bank

During the period of their phenomenal growth, credit bureaus have somehow escaped the focus of both state and federal inquiry and regulation in spite of the existence of serious abuses. For forty years only one state had legislation regulating the credit rating agencies,[23] and, in spite of growing consumer awareness, only five other states have passed similar legislation

---

[21] *See* Watwood v. Stone's Mercantile Agency, Inc., 194 F.2d 160 (D.C. Cir.), *cert. denied*, 344 U.S. 821 (1952); Bohlinger v. Germania Life Ins. Co., 100 Ark. 477, 140 S.W. 257 (1911); Petition of Retailers Commercial Agency, 342 Mass. 515, 174 N.E.2d 376 (1961); Hanschke v. Merchants Credit Bureau, 356 Mich. 272, 239 N.W. 318 (1931); Pollasky v. Minchener, 81 Mich. 280, 46 N.W. 5 (1890); Mitchell v. Bradstreet Co., 116 Mo. 226, 22 S.W. 358 (1893); Sunderlin v. Bradstreet, 46 N.Y. 188 (1871). Determining what this "interest" amounts to is a difficult task because, theoretically, anyone who had, has, or might have some dealings with the person in question could be said to have an "interest." The courts, however, have generally determined "interest" in terms of those who are furnished information in response to an inquiry submitted to the agency. *See, e.g.*, Erber & Strickler v. R.G. Dun Co., 12 F. 526 (C.C. Ark. 1882); Ritchie v. Arnold, 79 Ill. App. 406 (1898); Richardson v. Gunby, 88 Kan. 47, 127 P. 533 (1912); Hanschke v. Merchants Credit Bureau, 356 Mich. 272, 239 N.W. 318 (1931); Froslee v. Lund; State Bank, 431 Minn. 432, 155 N.W. 619 (1915). In King v. Patterson, 49 N.J.L. 417, 431, 9 A. 705, 712 (Ct. Err. & App. 1887), the court limited the scope of the privilege to communications with those having a "special interest." One court recently discounted general publication as grounds for loss of the privilege. *See* Stationers Corp. v. Dun & Bradstreet, Inc., 62 Cal. 2d 412, 398 P.2d 785, 42 Cal. Rptr. 449 (1965).

[22] *See* Johnson v. Bradstreet Co., 77 Ga. 172 (1886); *accord*, MacIntosh v. Dun, (1909) 18 A.C. 390 (P.C.); Pacific Packing Co. v. Bradstreet Co., 25 Idaho 696, 139 P. 1007 (1914). It has been recently suggested that strict liability, similar to products liability, be applied to credit agencies, reasoning that when the harm is concealed the incentive to produce safe, accurate products is absent. *See* Note, *Protecting the Subjects of Credit Reports*, 80 YALE L.J. 1035, 1054-61 (1971). *See generally* Plant, *Strict Liability of Manufacturers for Injuries Caused by Defects in Products—An Opposing View*, 24 TENN. L. REV. 938 (1957).

[23] *See* OKLA. STAT. tit. 24, § 81085 (1951) (enacted in 1910); 115 CONG. REC. S1163, S1166 (daily ed. Jan. 31, 1969).

within the past three years.[24] In effect, then, credit bureaus were a "quasi-public utility with virtually no public regulation."[25]

Congressional attention was brought to focus on credit bureaus as a result of legislative inquiries.[26] In 1961 the Bureau of the Budget commissioned a feasibility study for the centralization and computerization of the many personal records residing in individual agencies of the federal government for the purpose of making governmental recordkeeping and analysis more efficient and economical.[27] Four years later the committee issued the "Ruggles Report" which recommended that the Bureau of the Budget take immediate steps to establish a Federal Data Center.[28] Between July 26 and July 28, 1966, the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations held public hearings on the proposed data bank in order to study the potential erosions of the individual's right to privacy which might have been the ultimate result of such a venture.[29] The Special Subcommittee, under the chairmanship of Congressman Cornelius E. Gallagher, published its findings, conclusions, and recommendations in a report entitled "Privacy and the National Data Bank Concept" which was approved and adopted by the Committee on Government Operations exactly two years later on July 31, 1968.[30] The report expressed grave concern about

---

[24] ARIZ. REV. STAT. ANN. §§ 44-1691 to 44-1696 (Supp. 1970); CAL. CIV. CODE §§ 1750-57 (1973); MASS. GEN. LAWS ANN. ch. 93, §§ 44-46 (Supp. 1970); N.M. STAT. ANN. §§ 50-18-1 to 50-18-6 (Supp. 1969); N.Y. GEN. BUS. LAW §§ 370-76 (McKinney 1970).

[25] 115 CONG. REC. S1166 (daily ed. Jan. 31, 1969). Senator Proxmire stated further that

> [a]lmost every segment of the credit industry is subjected to detailed regulation, both State and Federal, to uphold the rights of the consumer. And yet the credit reporting industry, one of the most vital links in our credit system, has gone unregulated despite the existence of serious abuses. Under what theory of public policy can this anomaly be justified?

Id. *See also* 1968 U.S. CODE CONG. & AD. NEWS 1965-66.

[27] *See* H.R. REP. NO. 1842, 90th Cong., 2d Sess. 1 (1968).

[28] *See id.* at 1, 9. The "Ruggles Report" was so named after its chairman Richard Ruggles, professor of economics at Yale University. Two subsequent studies were conducted on the same topic and reports were developed: the "Dunn Report", by Edgar S. Dunn, of Resources for the Future, Inc., and the "Kaysen Report", by Dr. Carl Kaysen, chairman of the Institute for Advanced Study at Princeton University. Both agreed generally with the findings expressed in the "Ruggles Report", that is that a data center should be established. This recommendation was based in part on the tremendous amount of personal data on file with the various governmental agencies. At the time of the report, 67 million individual tax returns had been filed that year with the Internal Revenue Service, 22 million veterans' dossiers were on file in the Department of Defense and the Veterans Administration, and over 7.5 million individual resumes were on file at the U.S. Civil Service Commission.

[29] *See generally Hearings on the Computer and Invasion of Privacy Before a Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966).

[30] *See* H.R. REP. No. 1842, 90th Cong., 2d. Sess. (1968).

the potential harm such a system could cause to the privacy of individuals.[31] Concern about the misuse and possible inaccuracy of the data, coupled with skepticism about its security, led the Special Subcommittee to recommend that "no work be done to establish the data center until privacy protection was expanded more fully and guaranteed to the greatest extent possible . . . ."[32] Fortunately, the proposal itself was killed in committee.[33] It was at this time that members of the committee began to become aware of the existence of a "private data bank"—the credit bureaus.[34]

---

[31] *Id.* The Subcommittee found that:

1. The Ruggles and Dunn Reports recommend data center.
2. The Subcommittee notes possible threat to individual freedom posed by the National Data Bank concept.
3. Testimony indicated that data center information might be misused.
4. Need for limitations on types of data stored was demonstrated.
5. Kaysen Report recommends statutory provisions as sufficient to protect privacy.
6. Data center security would be more difficult than privacy protection in present agency systems.
7. Individual dossiers appear inevitable.
8. The citizen must have access to his own records.
9. The danger of unauthorized access to information is great.
10. Bureau of the Budget states National Data Center would be for statistical purposes only and supports advisory commission.
11. Bureau of Budget now considering specific proposals to submit to Congress.
12. Studies by professional group suggest improved federal statistical system may render National Data Bank concept irrelevant and unnecessary.

[32] *Id.* at 6. The Subcommittee recommended that:

1. . . .in the design and implementation of such systems the priority of privacy be asserted.
2. . . .that no work be done to establish the National Data Bank until privacy protection is explored fully and guaranteed to the greatest extent possible to the citizens whose records would form its information base.
3. . . .that the Bureau of the Budget, in formulating specific proposals for a National Data Bank, consider the proposals, safeguards and alternatives recommended by the Subcommittee.
4. The establishment of an independent supervisory commission.
5. . . .procedures to permit access to the National Data Bank by standing committees of Congress.

[33] Interview with Mr. Charles Witter, administrative assistant to Congressman Gallagher, March 1, 1972.

[34] This point was made by Congressman Gallagher during the testimony of Mr. W. Lee Burge, President, Retail Credit Co:

> At the rate [Retail Credit Co.] and the Associated Credit Bureaus are growing, I wonder whether all of this adds up to a very large national data bank, or national intelligence center in the hands of private industry.

Hearing on Retail Credit Co. of Atlanta, Ga., Before a Subcomm. on Invasion of Privacy of the House Comm. on Government Operations, 90th Cong., 2d Sess. 44-45 (1968) [hereinafter cited as *Hearings on Retail Credit Co.*].

Zablocki's Bill

One and a half months before Congressman Gallagher's subcommittee began its own investigation of these "private data banks" and almost seven months before the House Committee on Government Operations approved and adopted the Subcommittee's report on the National Data Bank, Congressman Clement J. Zablocki of Wisconsin introduced the first "Fair Credit Reporting Bill."[35] The bill was the result of a constituent's complaint about the treatment she had received from a credit bureau, and a survey which she had conducted on credit bureaus was attached to the letter.[36] The measure proposed by Zablocki would have given the consumer the right to know the identity of the credit rating agency, the contents of the report, and, in the case of an adverse report, the specific facts or allegations upon which the report was based. However, the existence and exercise of these rights would have hinged upon the consumer first requesting such disclosure of either the creditor or the credit reporting agency. The obvious assumption was that the consumer knew about credit reports and credit reporting agencies. This assumption was to be shown in later hearings to be without foundation.[37]

Zablocki's bill was referred to the House Committee on Banking and Currency,[38] but it was never reported out of the committee.[39] The bill, however, was effective if for no other reason than it inspired a number of similar proposals[40] and much congressional concern. It was also the original

---

[35]H.R. 15627, 90th Cong., 2d Sess. (1968).

[36]Interview with Ms. Margaret Goodman, administrative assistant to Congressman Zablocki, March 3, 1972. On September 6, 1967, Ms. Rita B. Collins wrote to the Congressman complaining that she had been turned down for a car loan because the credit agency erroneously reported that she and her husband owed money to a trucking firm. The rejection led to her own research of the problem in which, over a two-year period, she conducted interviews with more than 1000 individuals.

[37]*See* notes 64-71 *infra* and accompanying text.

[38]H.R. 15627, 90th Cong., 2d Sess. (1968).

[39]The major reason for this, given by Ms. Goodman, *supra* note 36, was that the Congressman was not on the Banking and Currency Committee and had little influence with the members of that Committee.

[40]A number of similar bills were introduced in Congress during 1968-69, but no hearings were held on these bills. 27 CONGRESSIONAL QUARTERLY 1160 (July 4, 1969) (Weekly Report). Congressman Patman introduced H.R. 15495 and Congressman Price introduced H.R. 10139 in 1968. In 1969 the following bills were introduced: H.R. 36; Congressman Tierman, H.R. 9888; Congressman Thompson, H.R. 9150; Congressman Helstroski, H.R. 7874; Congressman Diggs, H.R. 6747; and Congresswoman Sullivan introduced H.R. 16340. None of these bills, however, were directly coordinated with Congressman Zablocki's work, although most were very similar in focus and substance.

model for S. 823 which was eventually to become the Fair Credit Reporting Act.[41]

The Gallagher Hearings

On March 12, 1968, Congressman Gallagher's Subcommittee on Invasion of Privacy began the first of the many different committee hearings on the credit bureaus.[42] The Gallagher hearings were the cumulative result of the awareness of the problem caused by the work and study done on the National Data Bank and the thousands of letters and reports of cases received by Gallagher.[43] The four days of hearings only began to uncover the seriousness as well as the scope of the problem.[44] Gallagher recommended to the credit agencies that they join together and develop guidelines for self-regulation[45] which they did during the following months.[46]

Gallagher expected the credit industry to submit proposed guidelines during the summer so that further hearings could be held.[47] However, in early August, an article appeared in Life magazine which alleged in detail the corruption of Congressman Gallagher by the Mob in New Jersey and which referred to Gallagher as "the tool and collaborator of a Cosa Nostra gang lord, Joe Zicarelli."[48] The article was the culmination of an eight-month investigation of Gallagher's allegedly close connection with the Mafia. Con-

---

[41] 15 U.S.C. § 1861 *et seq.* (1970). Congressman Zablocki was to reintroduce this same bill a week after Senator Proxmire introduced S. 823.

[42] *See generally Hearings on Commercial Credit Bureaus, supra* note 1; *Hearings on Retail Credit Co., supra* note 34; *Hearings on the Credit Industry before the Subcomm. on Antitrust and Monopoly of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968); *Hearings on S. 823 Before the Subcomm. on Financial Institutions of the Senate Comm. on Banking and Currency*, 91st Cong., 1st Sess. (1969) [hereinafter cited as *Hearings on S. 823*]; *Hearings on 16340 before a Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 1st Sess. (1969).

[43] Interview with Mr. Charles Witter, *supra* note 33.

[44] The ostensible purpose of the hearings was to investigate the possible invasion of privacy on individuals who had applied for credit in making application for home loans. The Federal Housing Administration uses reports from credit bureaus to ascertain eligibility of mortgage applicants. Other federal agencies also use similar firms to run pre-employment checks. *See Hearings on Commercial Credit Bureaus, supra* note 1, at 1.

[45] Interview with Mr. Charles Witter, *supra* note 33.

[46] *See Hearings on Commercial Credit Bureaus, supra* note 1, at 141. Mr. John J. Spafford, executive vice-president, Associated Credit Bureaus of America, Inc., mentioned that the meetings were to begin within the next 30 days. Associated Credit Bureaus of America then organized a strategy meeting of 18-20 trade associations representing industries involved in one way or another with credit reporting. *See generally* Denny, *Federal Fair Credit Reporting Act*, 88 BANKING L.J. 579 (1971).

[47] Interview with Mr. Charles Witter, *supra* note 33.

[48] *See* LIFE, August 9, 1968, at 20-28.

sequently, his primary and immediate concern for sometime thereafter was, quite understandably, to protect his own good name.[49] No further hearings were held,[50] and it was not until January 13, 1969, nearly eight months after the hearings, that the credit industry submitted its guidelines.[51]

The Guidelines

Gallagher praised the guidelines and felt that further legislation would not be necessary even though he knew that Senator William Proxmire had already introduced a draft of his own bill to Congress five months earlier and would soon be introducing the bill itself. However, Gallagher was also aware that eventually Proxmire's bill would go to the House for approval and possible amendments.[52] For the industry, the drafting of the guidelines was more a point of political strategy than industrial ethics or concern. During the Gallagher hearings, the heads of the biggest credit reporting agencies in the country disagreed both as to whether legislation was necessary and, if necessary, what type of legislation was needed.[53] Politically, the industry's decision not to lobby against any proposed legislation but rather to issue self-regulating guidelines was an astute move on its part. Obviously, some regulation would be forthcoming. Self-imposed guidelines not only would be less restrictive than legislation, but would also show legislators—both state and federal—that the industry was willing and able to regulate itself, thus making statutory regulation unnecessary. Beneath this "good industry facade," however, was the more subtle benefit, namely, that self-regulation would impose no legal duties. Senator Proxmire, however, was highly critical of the proposed guidelines.[54] The basis for his criticism

---

[49]Interview with Mr. Charles Witter, *supra* note 33.

[50]Interview with Mr. Charles Witter, administrative assistant to Congressman Gallagher, February 18, 1972.

[51]*See* 115 CONG. REC. E198-99 (daily ed. Jan. 13, 1969).

[52]Interview with Mr. Charles Witter, *supra* note 33.

[53]Mr. W. Lee Burge, *supra* note 34, felt that no legislation was necessary, reasoning that the "competitive atmosphere" would be sufficient to insure accuracy and remedy the problems. *See Hearings on Retail Credit Co.*, *supra* note 34, at 45. Mr. H.C. Jordan, president, Credit Data Corp., disagreed, but felt that the only need for legislation was to prevent unauthorized access by either governmental agencies or private individuals. *See Hearing on Commercial Credit Bureaus*, *supra* note 1, at 96.

[54]*See* 115 CONG. REC. S1167 (daily ed. Jan. 31, 1969). Senator Proxmire criticized the guidelines for a number of reasons:

1. Not a single consumer organization participated in the development of the guidelines.

2. The guidelines were only recommendations. There was no assurance that they would be followed by the agencies.

3. No adequate means existed for the national trade association to enforce the guidelines.

was that the guidelines were unworkable, unenforceable, and not at all comprehensive as to the problems which needed to be remedied or the agencies which must be included.[55] Two and a half weeks after the guidelines were proposed and submitted to Congress, Proxmire submitted S. 823, his "Fair Credit Reporting Bill."

The Credit World—The Major Problem Areas

Before moving to a consideration of the Fair Credit Reporting Act, one must consider the problem areas in the credit world that were discovered in the above hearings. There are three general reasons for the initiation of a credit report: retail credit, personnel selection, and insurance. Retail credit ratings usually contain a person's address, family status, place of employment, approximate salary, credit history, where the applicant has charge accounts, and what his payment record has been. The file also contains information of public record such as court judgments, liens, indictments, and convictions.[56] The personnel credit ratings will include most of the same information as well as the applicant's employment record, his reasons for job changes, and remarks of former employers.[57] Insurance credit ratings are the type that draw the most stinging criticism since they usually contain information concerning the applicant's marital life, private morals, drinking habits, extra-marital affairs, and any tendency toward deviate sexual behavior.[58] The methods used to gather this type of information are less than reliable since they consist, for the most part, in nothing more than interviews with neighbors and friends of the applicant.[59] The basis, then, for a negative

---

4. Voluntary guidelines are inherently unstable and to a large extent unfair, mainly because they impose an added cost upon those who comply and give an unfair competitive advantage to those who do not.

5. Even if the guidelines were followed by all Associated Credit Bureaus of America members, approximately one-third of all credit bureaus do not belong to the association.

6. The guidelines do not cover firms engaged in insurance or personnel investigations where some of the most serious abuses and invasions of privacy have occurred.

7. The guidelines imposed no requirements on creditors or other users of information to disclose to consumers that they are being rejected because of an adverse credit report.

[55] Interview with Mr. Kenneth McLean, staff economist of the Senate Committee on Banking and Currency, March 24, 1972.

[56] *See Hearings on Commercial Credit Bureaus, supra* note 1, at 125; *Hearings on S. 823, supra* note 42, at 91.

[57] *Hearings on Commercial Credit Bureaus, supra* note 1, at 125; *Hearings on S. 823*, supra note 42, at 91.

[58] *See hearings on Retail Credit Co., supra* note 34, at 21; *Hearings on S. 823, supra* note 42, at 178.

[59] For a discussion of these methods of investigation see Sesser, *Big Brother Keeps Tabs on Insurance Buyers*, NEW REPUBLIC, April 27, 1968, at 11.

insurance credit rating is generally hearsay and malicious gossip, but also often includes value judgments of the applicant's life style.[60]

Given the virtually total lack of regulation of the "dossier industry"[61] as one critic has referred to it, problems concerning the collection of data and the maintenance of the files were generally unknown or ignored prior to the hearings on the credit industry. The hearings, although they have been referred to as "theatre,"[62] focused public attention and the congressional process on these and other problems and served to show the industry that Congress was serious in its concern as well as to document the abuses prevalent in the industry.[63]

One of the major problems identified during the hearings was the consumer's almost complete ignorance of the existence of credit reports.[64] The consumer is unaware that he is being damaged by an adverse credit report which may be so because of inaccurate or entirely false information.[65] The main reason for this ignorance is the standard agreements between credit reporting agencies and the users of their reports which prohibit the user from disclosing the contents of the report to the consumer.[66] As then written, these contracts typically bound the credit grantor to a conspiracy of silence.[67] The credit grantor was prohibited from disclosing to the applicant both the reason for refusal of credit and the identity of the agency which made the

---

[60]*See* 115 CONG. REC. S1164 (daily ed. Jan. 31, 1969); *Hearings on S. 823*, *supra* note 42, at 184, 194. Only Credit Data Corp., according to H.C. Jordan, *supra* note 53, had a strict policy of not including rumors or hearsay among the bits of information stored. He stated, however, that the computer could be set up to store anything. *Hearing on Commercial Credit Bureaus*, *supra* note 42, at 87.

[61]*See* Nader, *The Dossier Invades the Home*, SATURDAY REV., April 17, 1971, at 18-21.

[62]This reference was made by Mr. Howard Shuman, administrative assistant to Senator Proxmire, in a lecture at Georgetown University Law Center, April 11, 1972.

[63]Interview with Mr. Kenneth McLean, *supra* note 55.

[64]*See* S. REP. NO. 517, 91st Cong., 1st Sess. 3 (1969).

[65]*See* 115 CONG. REC. S1164 (daily ed. Jan. 31, 1969).

[66]*See id.* at S1164-65; Sesser, *Big Brother Keeps Tabs on Insurance Buyers*, NEW REPUBLIC, April 27, 1968, at 12. Until June 1968, the standard agreement for services included the following clause:

> All reports, whether oral or written, will be kept strictly confidential. Except as required by law, no information from reports [nor your identity as the reporting agency] will be revealed to the person reported on or to any other person except a person whose duty requires him to pass on the transaction in relation to which the report was ordered.

After June 1968, the bracketed section was omitted from the agreement. *Hearings on Retail Credit Co.*, *supra* note 34, at 47.

[67]*See* Comment, *Protection of the Consumer Interests and the Credit Rating Industry*, 2 PAC. L.J. 635, 641 (1971).

credit rating.[68] Unless the applicant knew that the reason he was being rejected for credit, insurance, or employment was because of a credit report, he had no opportunity to refute the "charges" against him.[69] Whether the consumer ever discovered the cause of his being rejected was largely a matter of an educated guess or clairvoyance bordering on blind luck.[70] It is interesting to note, as Senator Proxmire pointed out, that we certainly would not tolerate a government agency depriving a citizen of his livelihood or freedom on the basis of an unsubstantiated piece of gossip without an opportunity to present his side of the case. This kind of protected character assassination has no place in a democracy where the right of procedural due process is guaranteed to every citizen.[71] Yet, it was precisely this type of protection which the credit agencies enjoyed.

---

[68] *See* note 66 *supra* and accompanying text. *See also Hearings on S. 823, supra* note 42, at 189-90. Mr. W. Lee Burge, *supra* note 34, made an interesting comment during the hearings:

> We prohibit [disclosure] if at any stage of the complaint a man says where can I go to get this straightened out. Our contract would not allow [the user] to say go to Retail Credit Company, they are your problem. . . . [The consumer] finds his way to us in a large percentage of cases.

Hearings on Retail Credit Co., supra note 34, at 10.

[69] *See* S. REP. No. 517, 91st Cong., 1st Sess. 3 (1969).

[70] This particular point concerned members of the Subcommittee, especially Congressman Gallagher. The "vicious circle" aspect of such a policy was brought out quite clearly in an exchange between Congressman Gallagher and Mr. W. Lee Burge during the hearings on the Retail Credit Company:

> Gallagher: Suppose he isn't a very sophisticated fellow and he doesn't know about Retail Credit?
>
> Burge: It becomes more complex if a man doesn't known how to handle a problem of this sort, but generally speaking he has someone representing him, a salesman or an agent or someone who has his interests at heart. After he has had difficulty, someone usually says probably you ought to go to your credit bureau or the Retail Credit Co. or somebody to see if your problem is in the credit reporting area.
>
> Gallagher: He can't go to Retail Credit; he doesn't know Retail Credit is there.
>
> Burge: Somebody has just told him to come to Retail Credit Co.
>
> Gallagher: Then he breaks the contract because the contract says_____
>
> Burge: I don't know. Maybe the man who told him is not even a customer of ours.
>
> Gallagher: That is right, then he has to be just lucky.

Hearings on Retail Credit Co., supra note 34, at 45.

[71] 115 CONG. REC. S1163-64 (daily ed. Jan. 31, 1969). Professor Charles Reich, a professor of Law at Yale Law School, addressed himself to this same problem two years earlier:

> I think this is a denial of the constitutional right to confront, the constitutional right to face those who make statements about you, to question them, and to rebut, to answer. . .The truth, as lawyers know, is brought out in an atmosphere of adversary proceedings, of cross-examination, of being able to answer, to rebut. . . .Here are people who are not even charged with crime, and yet, who may be punished far more severely than the ordinary criminal. Here are people whose opportunity to have jobs, to earn money, whose reputations and everything else are about to be damaged forever, and they have no trial, no lawyer, no opportunity to find out anything. It

Credit agencies used the no-disclosure clause in their contracts supposedly to protect sources of information from "drying up."[72] Fearing that if sources knew they would be subject to later verification should the facts be challenged there would be a reluctance on their part to divulge information, the industry provided such protection with the idea that sources would speak more freely and candidly.[73] However, it became apparent that the primary purpose was to avoid the administrative burden as well as possible legal action should consumers become aware of and challenge the accuracy or veracity of the reports.[74]

In addition to the no-disclosure clause, credit agreements generally contained disclaimers of accuracy whereby the agency appears only as a transmitter of information.[75] The credit agency does not guarantee the accuracy, reliability, or correctness of the report. The disclaimer presents an added problem in that, despite its presence, the information in all probability will be taken as true unless there is reason for the subscriber himself to doubt its accuracy. There is, then, the possibility that those who receive the misinformation will act in reliance upon it, presuming it to be accurate.[76] In effect,

---

seems to me without question a denial of due process of law to send forth bad information about a person in secret in that way.

Hearings on the Computer and Invasion of Privacy Before a Subcomm. on the Invasion of Privacy of the House Comm. on Government Operations, 89th Cong., 2d Sess. 28 (1966).

[72]114 CONG. REC. S10030 (daily ed. Aug. 2, 1968).

[73]During the hearings on Retail Credit Co., Mr. Burge gave the rationalization of the policy in these words:

> It is a protection to the sources of information; it is a protection to the confidentiality of all the information because in reality much of the information that is reported is factual information but *it would result in the suppression of information* if each individual sought to correct his file in detail or sought to challenge a particular report in detail.

Hearing on Retail Credit Co., supra note 34, at 13 (emphasis added).

[74]*Id.*

[75]*See generally* 15 AM. JUR. *Collection & Credit Agencies* § 3 (1964). The standard Agreement for Services contract still contains such a disclaimer:

> We agree to hold you and your affiliate companies, and your and their officers, agents, employees, and independent contractors harmless on account of any expense or damage resulting from the publishing by us, our employees or agents of report information contrary to these conditions. Recognizing that information is secured by and through fallible human sources and that for the fee charged you cannot be an insurer of accuracy of any information furnished is not guaranteed by you, and we release you and your affiliated companies, and your and their officers, agents, employees, and independent contractors from any loss or expense suffered by us resulting directly from your reports or those of your affiliated companies.

Hearings on Retail Credit Co., supra note 34, at 47.

[76]*See* Note, *supra* note 3, at 262-63. One suggestion with considerable merit which has been proposed to help alleviate the financial burden is the possibility of third-party liability insur-

what was being done by the agencies and protected by judicial decision was to allow the honest communication of misinformation in order to insure the availability of correct information on occasion[77] even though the duty of the credit bureaus to subscribers was to furnish information which was accurate and not erroneous.[78]

A second major problem with the credit reports was that, even if a person knew the name of the credit reporting agency, he was rarely given access to the information in his file.[79] Insurance reporting firms generally would not even admit to having made a report on an individual much less reveal the contents of their files to him.[80] Credit bureaus would often place roadblocks in the path of the consumer who attempted to gain access to his file by placing a "nuisance charge" on the investigation or merely placing the date of the interview as much as two weeks away.[81] Yet access alone, without the

---

ance. The cost of such insurance could easily be passed onto the subscribers who, it would seem would willingly assume the extra cost (or pass it on to their own customers) in the interest of greater accuracy. The idea is by no means novel since many professions, the medical and legal being the best known, use the same type of insurance, and the services they perform are every bit as much in the public interest as those of credit bureaus. For a discussion of third-party liability insurance *see* Note, *Libel and Slander—The Qualified Privilege of Mercantile Agencies*, 9 S.C.L.Q. 291, 293 (1957).

[77] *See generally* Note, *supra* note 12, at 645.

[78] *See generally* Note, *Libel and Slander—The Qualified Privilege of Mercantile Agencies*, 9 S.C.L.Q. 291, 293 (1957).

[79] *See Hearings on Commercial Credit Bureaus*, *supra* note 1, at 10-11. The Subcommittee had addressed this same problem earlier when it investigated the National Data Bank. One of the findings of the Subcommittee, *supra* note 31, was that the individual must have access to his own files. The subcommittee reasoned:

> The best and most reliable way to assure that erroneous or non-contextual information is not stored in a National Data Center of any data system would be to allow each individual access to information concerning him.
>
> Even with restrictions on the type of material that can go into a data system and provisions for guaranteeing that only proper retrievals can be made, procedures should be established to allow an American the right to determine the nature of the information that could harm him. Electronic data processing need not, and must not, subvert the constitutional and legal safeguards Americans have the right to expect and demand.

H.R. REP. NO. 1842, 90th Cong., 2d Sess. 4 (1968).

[80] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 3 (1969).

[81] *Id.* Senator Proxmire, when introducing his bill, cited this as one of the major problems. By way of example, he cited to a credit bureau trade publication which stated:

> If the declined applicant is interested enough in his or her record to visit the bureau, and feels strongly enough that an error has been made, we should take the time to investigate. In checking with other bureau managers, I find most of them are willing to investigate. However, some bureaus discourage this by placing a nuisance charge on the investigation, or merely placing the date of the interview as much as two weeks away.

ability to correct or at least comment on a disputed item, is not a remedy; visibility does not necessarily correct problems.[82] Some credit bureaus proceeded on the assumption that the individual was guilty until proven innocent and refused to delete that which was no longer verifiable unless the consumer could prove it incorrect.[83] Since most credit agencies operate on a high-volume basis and correction procedures are costly, time spent with consumers going over individual reports would either reduce the agency's profits substantially or make the cost of the reports prohibitive.[84] The problem, then, would seem to be balancing the consumer's right to have only correct information in his credit report (and the user's right to correct information) against the agency's right to make a profit.[85] The question of whether good credit is actually a right or merely a privilege was never answered until the Fair Credit Reporting Act.[86]

The major criticism of the information contained in the reports was that it was often inaccurate. This inaccuracy included information which was false, incomplete, irrelevant, and obsolete.[87] Errors of identification are perhaps the most striking since they are so completely erroneous and unthinkable.[88] These errors arise because either the identifying information is the

---

115 CONG. REC. S1165 (daily ed. Jan. 31, 1969). This procedure, according to one investigator with Retail Credit Co. who asked to remain anonymous, is still continued today.

[82] *See* 115 CONG. REC. S1165 (daily ed. Jan. 31, 1969). As was pointed out during the hearings, Congressman Zablocki's original bill provided only for access and was silent as to the power to correct disputed data. *See Hearings on Commercial Credit Bureaus, supra* note, at 14.

[83] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 3 (1969).

[84] This point was made by Mr. W. Lee Burge during the hearings, when explaining the purpose behind the policy of the non-disclosure clause in the standard contracts:

> [J]ust because the legal processes are so involved and the time factor is so involved, we feel that the whole business information process would be slowed down and in many cases the cost would increase drastically because you are not preparing a case for trial when you make a business investigation. You are preparing the essentials for a decision on that particular transaction.

Hearings on Retail Credit Co., supra note 34, at 13. *See also* 115 CONG. REC. S1164-65 (daily ed. Jan. 31, 1969).

[85] Congressman Gallagher succinctly phrased the situation when he said, "Perhaps you are really selling people, merchandizing reputations, retailing character." *Hearings on Retail Credit Co., supra* note 34, at 45.

[86] *See* 115 CONG. REC. S1163, 1167 (daily ed. Jan. 31, 1969).

[87] *See id.* at S1163; 114 CONG. REC. S10029 (daily ed. Aug. 2, 1968). *See generally* Note, *supra* note 7; Miller, *Detour to 1984*, NATION, June 1, 1970, at 648-50 (general discussion of the quality of credit reports).

[88] During the hearings, it was admitted that about one percent of all reports involved mistaken identity. *Hearings on Commercial Credit Bureaus, supra* note 1, at 109. Although at first this may seem a negligible percentage, given the fact that over 110 million reports were issued, the error factor of 1.1 million is substantial.

same or so nearly the same as to make confusion inevitable unless a certain amount of care and precision is used. The Wall Street Journal carried an article a month before the Gallagher hearings describing how a New York assemblyman was refused a major credit card due to an "unfavorable" credit report, based, as he discovered after repeated phone calls, visits, and threats of legislative action, on an outstanding judgment against someone with a similar name.[89]

Credit files often contain incomplete information. Critics argue that this problem arises through the use of items of public record.[90] Credit bureaus systematically compile public record information such as records of suits, tax liens, arrests, indictments, convictions, bankruptcies, judgments, and the like. This information is taken from court records and newspaper accounts dealing with legal action involving individuals in the bureau's geographic area.[91] The information is then included in a person's credit report. The most serious flaw of this procedure is that the information is not kept current because to do so would be costly or because the information is not available.[92] Arrests can lead to dismissed charges; arrest records may be later expunged because the arrest was unjustified; lawsuits may also be dismissed or settled out of court; and convictions may be reversed on appeal. Yet this information rarely, if ever, gets recorded in the credit files. The prejudicial effect of reporting a civil or criminal action which has only been commenced is inherent especially when included in a report which will be used as the basis for credit or employment. Reliance upon the user's understanding that arrest does not equal guilt or that suit does not equal wrong is for the most part unfounded.

Biased reporting is a much more invidious form of inaccuracy. It can occur in two very different ways. A buyer and a seller may disagree over the quality of merchandise delivered or a tenant and landlord disagree over the conditions of the apartment rented. In both cases, the consumer may legally withhold payment to insure rectification of the alleged wrong. This tactic is the most effective leverage in getting performance of the contract as they believe it was made. What often happens, however, especially if heated words were exchanged, is that the seller or landlord will report this

---

[89] *See* Sesser, *How Credit Bureaus Collect and Use Data on Millions of Persons*, Wall Street Journal, Feb. 5, 1968, at 1. *See also Hearings on Commercial Credit Bureaus*, *supra* note 1, at 10-11.

[90] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969); *Hearings on Commercial Credit Bureaus*, *supra* note 1, at 10-11; 115 CONG. REC. S1164 (daily ed. Jan. 31, 1969).

[91] S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969); *Hearings on Commercial Credit Bureaus*, *supra* note 1, at 10-11; 115 CONG. REC. S1164 (Jan. 31, 1969).

[92] *See* Comment, *Protection of the Consumer Interest and the Credit Rating Industry*, 2 PAC. L.J. 635 (1971).

action simply as non-payment or slow payment.[93] This act of reprisal will hardly ever be discovered by the consumer although it will follow him in his credit report for many years. It is an anonymous treatment because the reporter of the information is never held accountable for it, and he is never in danger of defending a libel suit for having entered it. In addition, it allows for a good deal of slanderous, anonymous reprisal against purchasers on the part of some segments of the selling community.

The other form of bias is more subtle. It is the combination of the investigator's own value judgments and the "quota system." Based on his findings, regardless of how unfounded in fact they may be, the investigator must make a determination as to the subject's credit-worthiness. Influencing this decision is the factor that, prodded by supervisors trying to justify the service, the investigators are expected to file a certain percentage of derogatory reports.[94] Such a practice is reprehensible not only because of its arbitrariness, but also because of the inherent injustice it bespeaks. If credit reports are in fact an indispensible part of the new economic system, the minimum requirement should be that they be fair, impartial, and based on objective standards.

Credit reports often contain information which is either irrelevant or

---

[93] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 3 (1969); *Hearings on Commercial Credit Bureaus, supra* note 1, at 11; 115 CONG. REC. S1163-64 (daily ed. Jan. 31, 1969). The mechanics of this problem came to light in an exchange between Congressman Rosenthal and Mr. H. C. Jordan during the hearings:

> Rosenthal: Let's suppose a television set that I bought on credit doesn't work well and I tell them that I am not going to pay until the set is fixed or replaced, and I don't pay for 2 or 3 months and we have this dispute going, what happens to my credit rating?
>
> Jordan: If you refuse to pay for the television set, the subscriber's accounting system, unless he inhibits it, will record the fact that you are 60 days delinquent. This is a fact of your credit experience.
>
> Rosenthal: So because of the fact that he sold me a bum television set I can't go out and get a mortgage and buy a new house?
>
> Jordan: Whether you can get a mortgage depends on the mortgage lender's interpretation.
>
> Rosenthal: The mortgage lender from reading your record would not know that I am a pretty good guy but there is this dispute over a television set; he would get a piece of cold information that would have marked me as a delinquent.
>
> Jordan: He would have the facts which are undeniable that you did not pay your bill.

Hearings on Commercial Credit Bureaus, supra note 1, at 76.

[94] *See* Nader, *The Dossier Invades the Home*, SATURDAY REV., April 17, 1971, at 19; TIME, May 3, 1971, at 86 (stating that the rejection rate often runs as high as 10-15 %). Generally, credit agencies report that the rejection rate ("unfavorable reports") is about five percent. *See Hearings on Retail Credit Co., supra* note 34, at 25.

obsolete or both.[95] Information about a person's private life, such as racial or ethnic descent, domestic trouble, housekeeping habits, or the condition of his yard are basically irrelevant for purposes of deciding credit-worthiness or suitability for employment. Such information is generally based on subjective opinion rather than objective fact and may even invade the individual's right to privacy.

Obsolete information is a different problem mainly because creditors obviously have a right to know if a person had a history of bill-paying troubles or a pattern of bankruptcies. It would seem unfair, however, to burden a consumer with a bad-credit rating for life, especially since the basis for the rating may have been one or more of the inaccuracies discussed above. Some agencies have a regular review and destruction process, but others do not.[96]

The confidentiality of credit reports is another major concern.[97] Until recently, credit reporting agencies had only a vague policy as to when they would furnish information. Unauthorized access to the highly personal information, some of which may have been inaccurate, was only one aspect of the problem. The point was well demonstrated by Professor Alan Westin during the Gallagher hearings.[98] Information on the personal background of

---

[95] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969). The Federal Trade Commission has stated in an advisory opinion that there is no restriction as to relevancy in the Act. *See* 4 CCH CONSUMER CREDIT GUIDE ¶ 11,313, at 59,806 (1971).

[96] *See* S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969). Mr. W. Lee Burge acknowledges that Retail Credit Co. reviews its files yearly, deleting everything which does not have an immediate value:

> We determine whether there is serious fraud situation or a claim history or something, bankruptcy or criminal record or something along that line that should be retained for a period longer than 13 months. Most of the files which we have are destroyed in less than two years.
>
> Wydler: You mean they are physically destroyed?
>
> Burge: We tear them up and throw them away.
>
> Wydler: This is not a case of crossing out things on old reports? You actually take the report and dispose of it?
>
> Burge: It is not a deletion of out-of-date information. It is a destruction process.
>
> Gallagher: Do you keep adverse information?
>
> Burge: We keep adverse information there depending on its seriousness. But most adverse information is destroyed within a five-year period.

Hearings on Retail Credit Co., supra note 34, at 30-31.

[97] *See* 115 CONG. REC. S1165-66 (daily ed. Jan. 31, 1969); 114 CONG. REC. S10,030 (daily ed. Aug. 2, 1968); *Hearings on Commercial Credit Bureaus, supra* note 1, at 1. This same problem was focused upon by the Subcommittee during the hearings on the National Data Bank and became a major finding. *See* H.R. REP. NO. 1842, 90th Cong., 2d Sess. 3-9 (1968).

[98] For a more detailed discussion of the experiment see *Hearings on Commercial Credit Bureaus, supra* note 1, at 6-10. S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969), refers to another experiment conducted by a reporter for a major TV network who was able to obtain ten out of twenty reports requested at random from twenty credit bureaus by using the name of a completely fictitious company under the guise of offering the individuals credit.

one of his assistants was freely and quickly furnished despite the fact that Columbia University was neither a credit grantor nor a member of the local bureau. These "favor reports" are not, in many instances, connected with any legitimate business need.[99] This is in direct contradiction to the stated policy of credit bureaus "to set the highest priority on the protection of the rights and best interests of the individual."[100] Facades of concern and statements of sincerity may abate criticism but are easily seen for what they are by investigating daily business practices. It is interesting to note that in the statement of the basic philosophy of credit bureaus nowhere are the needs of business counter-balanced by the individual's right to privacy.[101] Once an individual's name gets into the files, he has no power to control the access to the information contained therein. This problem has been turned aside by the assumption that once a person applies for credit, his consent to investigation is implied.[102] This is difficult to understand because most, if not all, of the time the individual is completely unaware of the existence of the files. The mental gymnastics of implied-consent-equals-implied-authorization is subtle at best, especially since in reality much access is unauthorized.[103]

A second aspect of the problem of confidentiality is the accessibility to the files by the State Department, the Federal Bureau of Investigation, and other federal agencies as a standard practice.[104] A number of agencies in the government make loans under conditions which would indicate the necessity for utilizing the services of credit bureaus.[105] Such a practice would most

---

[99]*See Hearings on Retail Credit Co., supra* note 34, at 37-38.

[100]*See id.* at 5.

[101]*See* 115 CONG. REC. S1165 (daily ed. Jan. 31, 1969).

[102]*See Hearings on Commercial Credit Bureaus, supra* note 1, at 116.

[103]One of the methods of checking such unauthorized access would be to require credit agencies to keep a record of all who have had access to the file or who have received information from the agency. This recommendation was made during the hearings by Professor Alan Westin. *See Hearings on Commercial Credit Bureaus, supra* note 1, at 14-15.

[104]*See* Sesser, *Big Brother Keeps Tabs on Insurance Buyers*, NEW REPUBLIC, April 27, 1968, at 11.

[105]A number of agencies, by statute, fall into this category:

Export-Import Bank of Washington—12 U.S.C. §§ 635 *et seq.* (1970).

Farm Credit Association—12 U.S.C. §§ 641 *et seq.* (1970).

Federal Deposit Insurance Corporation—12 U.S.C. §§ 1811 *et* seq. (1970).

Federal Home Loan Bank Board—12 U.S.C. §§ 1437, 1701c(b) (1970).

Department of Health, Education and Welfare (Public Health Service)—42 U.S.C. §§ 294 *et seq.* (1970).

Department of Interior, Bureau of Commercial Fisheries—16 U.S.C. §§ 742A *et seq.* (1970).

Department of State (Agency for International Development—22 U.S.C. §§ 2151 *et seq.* (1970).

Veterans Administration—38 U.S.C. §§ 210 *et seq.* (1970).

probably fall within the "legitimate business need" rule, a prerequisite for publication and disclosure. The necessity of employing an outside data-gathering organization in order to expedite federal loan programs is understandable only within this context. Use of credit agencies as an alternative investigative arm of the federal government, however, is in direct opposition to the established purpose and philosophy of credit agencies. The government's right to investigate is not absolute and is subject to various constitutional restraints including the guarantee of the fourth amendment against unreasonable search and seizure. Neither the government nor the credit agencies have been concerned with protecting these basic rights of citizens. The government does not bother to obtain search warrants, and credit bureaus rationalize disclosure as their "voluntary co-operation with these agencies to be in the public interest."[106] Congressman Gallagher correctly remarked that "[w]hat we are really reaching is a total surveillance society and a totally managed society . . . ."[107]

The anticipated computerization of the credit agencies' files has caused increasing concern.[108] The possibility of a national file of credit information available to any subscriber in a matter of seconds is both remarkable and frightening. Computer errors are common and unpredictable.[109] Additionally, the myth of computer infallibility still prevails. Computer systems often spew forth incorrect data and half-truths which, because of the overwhelm-

---

[106] *See Hearings on Retail Credit Co., supra* note 34, at 23. The comments of Mr. W. Lee Burge on this point are interesting:

> In this respect we have acted on the advice of counsel that there is no legal prohibition against such voluntary cooperation in lieu of insisting that a subpoena, search warrant, or other comparable legal procedure be followed by the Government investigators. We have considered our voluntary cooperation with these agencies to be in the public interest.

Id. (emphasis added). From the testimony, it is evident that Mr. Burge failed to realize that contained within this "legal" procedure is a burden upon the Government to show cause, and, should they be unable to show cause for such an order, the privacy of the individual is given precedence over the Government's desire to investigate. *See also id.* at 133.

[107] *Id.* at 136. Gallagher's further comments were even more harsh:

> You may be right if we become a total surveillance society. I personally think a managed society with total surveillance differs little from Hitler's Germany. Now we can have computerized nazism [*sic*] if we are not careful.

[108] *See* 115 CONG. REC. S1164 (daily ed. Jan. 31, 1969); 114 CONG. REC. S10,029 (daily ed. Aug. 2, 1968).

[109] *See* 115 CONG. REC. S1164 (daily ed. Jan. 31, 1969); H.R. REP. NO. 1842, 90th Cong., 2d Sess. 30-34 (1968), discusses the Comptroller General's Report to the Congress—Review of Reliability of the Air Force's Personnel Data System, B-164471, July 25, 1968. The report pointed up serious inadequacies including failure of the system to sustain an acceptable error factor. By way of analogy, if an experimental high-priority system could not be maintained with a guarantee of reasonable accuracy, chances are much less that a private data system would perform any better.

ing incomprehensibility of such complex systems on the part of outsiders, are accepted as irrefutable dogmatic pronouncements. Anyone who has attempted to argue with a computer knows true frustration.

Errors in programming or resulting from "debugging" are only one aspect of the problem. Security is also a crucial concern.[110] Various techniques can be employed in order to make the data contained in the files more difficult to acquire. However, if the purposes of computerization are to be fulfilled, the security procedures cannot be too complex because access must be had by all participating agencies. No cryptographic code is ever considered foolproof; it merely delays unauthorized access.[111] With access keys available to all agencies sharing the system, the chances of security being breached are much greater. As the science of electronics continues to advance and the discoveries made are improved upon, if not made obsolete, even before they are marketed, the need for safeguards becomes more crucial if the right of privacy of the individual is to have any meaning.[112]

The Right to Privacy

The growing need for some congressional action in the credit world was paralleled by the growing judicial concern for developing a right to privacy. The right to privacy or the "right to be left alone"[113] has developed during the past fifty years to the point that today it is practically a household word. Yet, as one writer recently observed:

> "Privacy" is fast becoming a word like "ecology"; it is something everyone favors but is nonetheless regarded as an abstraction that can be eroded in favor of more immediate or "realistic" objectives:

---

[110]*See* H.R. REP. No. 1842, 90th Cong., 2d Sess. 3-4 (1968).

[111]*See id.* at 19. Referring to the "Dunn Report", the Subcommittee noted that since all material about an individual would be stored in one place, the reward for each act of snooping would be much greater than at present . . . It is probable that advances in electronic surveillance will continue to outpace advances in protective devices. . . .

Id.

[112]One of the more startling advances has been in the area of inferential relational retrieval techniques which are now being developed. Such techniques, when fully refined, could determine relationships of any person, organization, event, etc., to any other person, organization or event. *Id.* at 20.

[113]Judge Cooley in 1888 coined the phrase "the right to be let alone." *See* COOLEY, TORTS 29 (2d ed. 1888). *See also* 1 HARPER & JAMES, THE LAW OF TORTS § 9.6, at 681 (1956). Invasion of privacy is actionable in all but four states. *See* Brunson v. Ranks Army Stores, 161 Neb. 519, 73 N.W.2d 803 (1955); Henry v. Cherry & Webb, 30 R.I. 13, 73 A. 97 (1904); Milner v. Red River Valley Pub. Co., 249 S.W.2d 227 (Tex. 1952); Yoeckel v. Samonig, 272 Wis. 430, 75 N.W.2d 925 (1956).

> crime control, national security and the necessity to maintain "complete" data. And like ecology, its purposes will never be served so long as it is regarded as the exclusive concern of Congress or the courts.[114]

Just as ecology means more than cleaning up polluted streams and smog-dense air, so too privacy means more than being "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[115] As one author described it, "the invasion of privacy should more accurately be called the invasion of self. The right to protect oneself from informational assault is basic to the inviolability of the individual."[116] Informational assault is a relatively recent phenomenon primarily because it was never a real possibility until the computer had acquired a certain degree of sophistication.[117] Comparisons between various computer development stages are referred to as "generations" because the advancements are so major.[118] It is understandable, therefore, that the ordinary man tends to ignore that which may eventually become his greatest threat to privacy. The threat arises not so much from invasion in the normal "physical" sense, but from the computer's capacity to store a fantastic amount of data on an individual and to retrieve and transmit it to anyone with an access key.

The problem of controlling this information is central to a discussion of privacy in the context of information usage. One author described privacy as

> that aspect of social order by which persons control access to information about themselves . . . . The concept of privacy requires a sense of control and justified acknowledged power to control aspects of one's environment. Privacy is not just an ab-

---

[114]Schrag, *Dossier Dictatorship*, SATURDAY REV., April 17, 1971, at 25.

[115]U.S. CONST. amend IV.

[116]Nader, *The Dossier Invades the Home*, SATURDAY REV., April 17, 1971, at 59. *See generally* A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971).

[117]Professor Alan Westin's description of the future trend in data surveillance indicates the immediate and crucial need for a complete and totally objective re-evaluation of the evolutions of data retrieval systems and implication of such systems for the future. He describes the "laser memory process" whereby on one 4800-foot reel of one-inch plastic tape twenty pages of information on every man, woman, and child in the United States can be stored in digital form. The extent of the information that could be contained on ten or a hundred such reels staggers the imagination. *See* A. WESTIN, PRIVACY AND FREEDOM 163-68 (1967).

[118]Ms. Jane Kadish, a former computer expert for the Department of Health, Education and Welfare, recently remarked to the author that "the computer is the only machine that is obsolete by the time it hits the market."

> sence of information about ourselves; it is the feeling of control over that information.[119]

Only recently did Congress become aware of the potential erosion of the individual's right to privacy.[120] Lately this has been expanded to include the "consumer's right of privacy."[121] As Senator Proxmire stated: "At some point the individual's right to privacy must take precedence over the creditor's right to obtain information."[122] In fact, the restriction on reporting highly personal information as an unjustifiable invasion of privacy was originally within the scope of the legislation when the hearings were held.[123]

Informational privacy is only the latest of the many aspects of privacy which the courts and commentators are beginning to view as a recognizable right.[124] One can control one's right to privacy only if one can control the interference with one's life. This is accomplished by continually redefining the growing fringes of the first ten amendments. The penumbra of the first amendment, where privacy is protected from government intrusion, was recognized in *NAACP v. Alabama* where the Supreme Court protected the "freedom to associate and privacy in one's associations."[125] Without the peripheral right to educate a child in a school of the parents' choice[126] or the peripheral right to study a foreign language[127] the specific rights of the first amendment would be less secure.[128]

In *Griswold v. Connecticut* Justice Douglas, writing for the Court, defined the right to marital privacy and said that "specific guarantees in the Bill of

---

[119]Freid, *Privacy*, 77 YALE L.J. 475, 493 (1968).

[120]*See* H.R. REP. NO. 1842, 90th Cong., 2d Sess. (1968).

[121]*Hearings on S. 823, supra* note 42, at 74, 82. *See also* Note, *supra* note 7; S. REP. NO. 517, 91st Cong., 1st Sess. 4 (1969).

[122]TIME, May 3, 1971, at 87 (quoting Senator William Proxmire).

[123]H.R. REP. NO. 16,340, 91st Cong., 2d Sess. 54 (1970). It was originally proposed that the industries be restricted to reporting only information "reasonably relevant" to the purpose for which the report was to be used. *See also* Note, *The Fair Credit Reporting Act*, 56 MINN. L. REV. 819 (1972).

[124]*See* Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUMAN RIGHTS L. REV. 1 (1972). Considering today's technology, perhaps it is the computer which has too much privacy. One U.S. Senator has recently suggested that the Congress, the press, and the public should have available to them a habeas corpus action for entire computer systems and programs. If not lawful and relevant, the systems should be exposed for what they are—attempts to intimidate citizens into silence and conformity. *See* Ervin, *The First Amendment: A Living Thought in The Computer Age*, 4 COLUM. HUMAN RIGHTS L. REV. 13, 42 (1972).

[125]357 U.S. 449, 462 (1958).

[126]Pierce v. Society of Sisters, 268 U.S. 510 (1925).

[127]Meyer v. Nebraska, 262 U.S. 390 (1923).

[128]Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[129] The right to privacy is not new. What is new is the expansion of the concept. Various guarantees create zones of privacy. The right of association is within the first amendment; the third amendment is another facet of that privacy. The fourth amendment affirms the right to privacy against unreasonable searches and seizures; the fifth amendment gives a person a zone of privacy which government may not force him to surrender to his detriment; and the ninth amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[130] Concurring in *Griswold*, Justice Goldberg differed with the majority in that his conception of personal liberty and rights reserved under the ninth amendment encompassed the right to marital privacy, and obviated the necessity of pinning that right to penumbral emanations of other specific constitutional guarantees.[131]

The Supreme Court, in its recent decision on the question of abortion, has defined a new aspect of privacy. The Court held that the right to privacy, whether based on the fourteenth amendment's concept of personal liberty or on the ninth amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.[132] In a concurring opinion, Justice Douglas recites a catalogue of those "certain rights . . . retained by the people" in the ninth amendment which includes

> customary, traditional, and time-honored rights, amenities, privileges, and immunities that come within the sweep of "the Blessings of Liberty" mentioned in the preamble to the Constitution.[133]

He then proceeded to set out those rights which come within the meaning of the term "liberty" as used in the fourteenth amendment. First, is the individual's control over the development and expression of his intellect,

---

[129] *Id.* at 484.

[130] *Id.* For the Court's discussion of these penumbral rights of privacy and repose see Wyman v. James, 400 U.S. 309 (1971); Stanley v. Georgia, 394 U.S. 557 (1969); Katz v. United States, 389 U.S. 347 (1967); See v. Seattle, 387 U.S. 541 (1967); Camara v. Municipal Court, 387 U.S. 523, 528 (1967); Lanza v. New York, 370 U.S. 139 (1962); Monroe v. Pape, 365 U.S. 167 (1961); Frank v. Maryland, 359 U.S. 360 (1959); Public Utilities Comm'n v. Pollak, 343 U.S. 451 (1952); Rochin v. California, 342 U.S. 165, 172 (1952); Breard v. Alexandria, 341 U.S. 622, 626 (1951); Skinner v. Oklahoma, 316 U.S. 535, 541 (1942); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616 (1886).

[131] 381 U.S. at 486-99.

[132] Roe v. Wade, 93 S.Ct. 705 (1973).

[133] 93 S. Ct. at 757.

interests, tastes, and personality.[134] Second, is freedom of choice in the basic decisions of life involving marriage, divorce, procreation, contraception, and the education and upbringing of children.[135] Third, is the freedom to care for one's health and person, to be free from bodily restraint or compulsion, and to walk, stroll, or loaf.[136]

As new zones of privacy are defined, we are reminded of Justice Brandeis' dissenting opinion in *Olmstead v. United States:*

> The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[137]

Yet, as informational privacy is gaining recognition, collected information is only one aspect of the threat to that privacy. The method in which it is gathered is as great a concern, and it is to this problem which the Fair Credit Reporting Act addresses itself.

The Fair Credit Reporting Act

On August 2, 1968, Senator William Proxmire introduced a draft of the

---

[134]*See, e.g.*, United States v. Van Leeuwan, 397 U.S. 249, 253 (1970); New York Times Co. v. Sullivan, 376 U.S. 254, 293 (1964) (Black, Douglas, JJ., concurring); Kingsley Pictures Corp. v. Regents, 360 U.S. 684, 697 (1958) (Douglas, J., concurring); Roth v. United States, 354 U.S. 476, 508 (1957) (Douglas, J., dissenting); Watkins v. United States, 354 U.S. 178, 196-199 (1957); Terminiello v. Chicago, 337 U.S. 1 (1948). Justice Douglas views these rights which are protected by the first amendment as absolute, permitting of no exceptions. Roe v. Wade, 93 S. Ct. 705, 757 (1973) (Douglas J., concurring).

[135]*See, e.g.*, Eisenstadt v. Baird, 405 U.S. 438 (1972); Kramer v. Union Free School Dist., 395 U.S. 621 (1969); Shapiro v. Thompson, 394 U.S. 618 (1969); Loving v. Virginia, 388 U.S. 1 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); Carrington v. Rash, 380 U.S. 89 (1965); Sherbert v. Verner, 374 U.S. 398 (1963); NAACP v. Alabama, 357 U.S. 449 (1958); Kent v. Dulles, 357 U.S. 116, 126 (1958); Skinner v. Oklahoma, 316 U.S. 535 (1942); Pierce v. Society of Sisters, 268 U.S. 510 (1925). Justice Douglas views these rights as fundamental, and, in order to support some legislative control of them, a statute must be narrowly and precisely drawn, and a "compelling state interest" must be shown to support a limitation. Roe v. Wade, 93 S. Ct. 705, 758 (1973) (Douglas, J., concurring).

[136]Papachristou v. City of Jacksonville, 405 U.S. 156, 164 (1972); Terry v. Ohio, 392 U.S. 1, 8-9 (1968); Katz v. United States, 389 U.S. 347, 350 (1967); Meyer v. Nebraska, 262 U.S. 390, 399 (1923); Jacobson v. Massachusetts, 197 U.S. 11, 29, (1905); Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 252 (1891). Justice Douglas states that these rights, while also fundamental, are subject to regulation on a showing of "compelling state interest". Roe v. Wade, (93 S. Ct. 705, 758 (1973) (Douglas, J., concurring).

[137]277 U.S. 438, 478 (1928).

Fair Credit Reporting Bill.[138] The bill was first presented in its skeletal form for the stated purpose of bringing it to the immediate attention of the other members of Congress so that they might give it serious consideration and focus in on the issues and problems it was designed to correct.[139] Consumer issues were an important and appealing political concern, especially after the Gallagher hearings exposed some of the serious, yet heretofore unknown, problems dealing with credit reporting. The advantage of imposing uniform regulation through congressional action was obvious. The need, at least insofar as the consumers were concerned, was immediate. Having recently passed the Consumer Credit Protection Act,[140] Congress had a perspective from which to evaluate problems dealing with the broad topic of credit as well as an interest in the specific area of credit reporting. In a certain sense the time was right.

Senator Proxmire had become aware of the problem of credit reporting while working toward passage of the Truth in Lending Act.[141] This experience was supplemented by correspondence he received during that time which pointed to other consumer credit problems. The draft of the Fair Credit Reporting Bill included only major areas and objectives because of a lack of specific expertise in the area, in spite of the Gallagher hearings, as well as a desire for as much constructive input as possible. Proxmire had hoped that this input would be the result of hearings which he wanted to conduct later that same year. However, these hearings never materialized because the new Congress was more concerned with other matters.

In the interim, Senator Philip Hart held two days of hearings on the credit industry in mid-December.[142] He was then chairman of the Subcommittee on Antitrust and Monopoly which was used as an effective forum for investigating and documenting abuse under the guise of considering the possible antitrust implications of credit agencies being controlled by a handful of people.[143] The testimony and the witnesses were basically repeats of the Gallagher hearings. The subcommittee held hearings again in January of the following year. However, no legislative action was forthcoming.

During the same month, Gallagher presented to Congress the self-

---

[138] *See* 114 CONG. REC. 10031 (daily ed. Aug. 2, 1968).

[139] *See id.* at 10029.

[140] 15 U.S.C. § 1601 *et seq.* (1970) (effective May 29, 1968).

[141] Much of the information which follows was obtained from an interview with Mr. Kenneth McLean, staff economists for the Senate Committee on Banking and Currency, March 24, 1972.

[142] *See Hearings on the Credit Industry Before the Subcomm. on Antitrust and Monopoly of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968).

[143] 27 CONGRESSIONAL QUARTERLY 13 (January 3, 1969) (Weekly Report).

regulating guidelines developed by the Associated Credit Bureaus.[144] As mentioned above,[145] Proxmire criticized the guidelines as being practically useless. In effect, they provided too little too late. Two weeks later Proxmire introduced S. 823, the Fair Credit Reporting Bill.[146] It differed in only a few respects from the draft submitted on August 2, 1968. Excluded from the bill was a long list of definitions which was later to be expanded in the Act.[147]

S. 823 expanded one section of the draft and added two new sections, all of which were designed to meet head-on some of the major problems that surfaced during the hearings on the credit industry. The original section on "Prohibitions" limited the dissemination of credit information and prohibited it unless procedures insuring confidentiality and providing for notification and access were established.[148] This section was included in S. 823 under the title "Requirements of credit rating agencies." It more narrowly limited the scope of the data collected and retained, permitting it to be furnished only to persons with a "legitimate business need."[149] The Act outlined the permissible use of reports in greater specificity, but also included allowances for its release pursuant to a court order or at the request of the consumer.[150] The Act also included a special section limiting the access which governmental agencies could have to the files.[151]

S. 823 included a section (not part of the original draft) which required the user of a credit report who denies credit to a consumer wholly or partly because of the report to so inform the consumer and supply the name and address of the credit reporting agency which made the report.[152] The Act went one step further by requiring the user to inform the consumer that a report *may* be prepared and that the consumer has a right to request additional disclosures.[153] The Act further defined the procedures and conditions

---

[144]115 CONG. REC. E198-99 (daily ed. Jan. 13, 1969).

[145]*See* notes 54-55 *supra* and accompanying text.

[146]115 CONG. REC. S1168 (daily ed. Jan. 31, 1969).

[147]*Compare* § 502 of the draft *with* § 163 of S. 823 *and* § 1681a of the Act.

[148]*See* § 503(2) of the draft. 114 CONG. REC. S10031 (daily ed. Aug. 2, 1968).

[149]*See* § 164(c), (f)(1) and (f)(2) of S. 823. 115 CONG. REC. S1168 (daily ed. Jan. 31, 1969). The Senate bill was subsequently criticized for allowing market researchers, detective agencies, lawyers, and various investigative groups access to the file. *See* Miller, *The Credit Networks, Detour to 1984*, NATION, June 1, 1971, at 669.

[150]*See* 15 U.S.C. § 1681b (1970). In 15 U.S.C. § 1681e (1970), the Act also outlined the required compliance procedures so as to avoid unauthorized access.

[151]15 U.S.C. § 1681f (1970). This information is limited to identifying information such as his name, address, former addresses, place of employment, or former places of employment.

[152]*See* § 165 of the bill. 115 CONG. REC. S1168 (daily ed. Jan. 31, 1969).

[153]15 U.S.C. §§ 1681d, 1681m (1970). These sections, like others, have been narrowly interpreted by various agencies. An example of the standard notification is that of New England Mutual Life Insurance Co.:

of disclosure as well as the type of information to which the consumer will have access.[154]

S. 823 included one other section not contained in the draft—one which would give the consumer a remedy for any willful noncompliance. This section dealt with "civil liability" and allowed the consumer to collect actual damages sustained as a result of noncompliance by a user or a credit reporting agency, reasonable attorney fees, and punitive damages within a range of $100-$1000 at the discretion of the court.[155] In addition, the section conferred jurisdiction upon federal courts and imposed a two-year statute of limitations which would begin to run at the date of the occurrence of the violation.[156] This section, however, in effect, did little more than codify existing case law. The burden on the consumer of showing "willful noncompliance" would have been nearly as impossible as showing "actual malice" which was generally required previously.[157] By making intent an element of the violation, S. 823, for all but a very few instances, would have given a right without anything more than a hollow remedy.

This problem was recognized, and the Act made a distinction between "willful noncompliance"[158] and "negligent noncompliance."[159] The section in the Act dealing with willful noncompliance was the same as that contained in S. 823, with one important exception: the range of punitive damages which the court could allow was omitted. This was a significant change because it allowed the punitive damages to be just that, thereby providing an effective deterrent. It could reasonably be questioned that the $100-$1000 range of damages allowed by S. 823 would have been punitive or would have provided any deterrence factor.

An investigation has been requested. It is a routine investigation made in connection with almost all applications for life insurance and includes such general identification information as residence verification, marital status, number of children, occupation, employment, general health, habits, reputation and mode of living, obtained through personal interviews.

Consumer Report Letter from New England Mutual Life Insurance Co. to the author, June 15, 1971.

[154] 15 U.S.C. §§ 1681g, 1681h (1970). The Act requires that the nature and substance of all information (except medical information) in its files at the time of the request be disclosed to the consumer. It also provides for the disclosure of the sources of information except when these sources were acquired solely for use in preparing an investigative report. The agencies must also disclose the names of those who had received reports within a certain stipulated time depending upon the purpose of the report.

[155] *See* § 166(a) (1)-(3) of S. 823. 115 CONG. REC. S1168 (daily ed. Jan. 31, 1969).

[156] Id. at § 166(a)(4).

[157] *See* note 16 *supra* and accompanying text.

[158] 15 U.S.C. § 1681n (1970).

[159] 15 U.S.C. § 1681o (1970).

In addition to providing the consumer with a remedy against the credit agency and the user for willful noncompliance, it also provided for actual damages and attorney's fees for negligent noncompliance. The Act also went two steps further. It provided substantial penalties against any person who knowingly and willfully obtains information on a consumer from a credit agency under false pretenses[160] and against any officer or employee who knowingly and willfully provides information concerning an individual from an agency's files to a person not authorized to receive such information.[161] However, the penalties are criminal in nature and allow no recovery by the consumer in the way of damages.[162]

The Act makes the same provision for jurisdiction as did S. 823 except that, in cases of material and willful misrepresentation of *any* information, the two-year statute of limitations does not begin to run until such misrepresentation has been discovered by the consumer.[163] The difficulty of proving intent and materiality is great, but the section at least provides the consumer with a significant legal advantage should such a situation occur.

On February 4, 1969, Congressman Zablocki again introduced his version of the Fair Credit Reporting Bill. However, no action was taken in the House Committee mainly because of his limited influence with its members.[164] Had he been more forceful a personality, he might have been able to persuade Congressman Patman, the Committee chairman, to act on the bill, but this was not the case.[165] In general, S. 823 went far beyond the provisions of H.R. 6071, which was virtually the same bill introduced by Zablocki the year before.

Senator Proxmire began his hearings on S. 823 on May 23, 1969.[166] Much

---

[160]15 U.S.C. § 1681q (1970). This section provides for penalties up to $5000, or one year in prison, or both.

[161]15 U.S.C. § 1681r (1970). This section provides for fines up to $5000, or one year in prison, or both.

[162]One point worth noting is that it would seem that 15 U.S.C. § 1681q (1970), *see* note 145 *supra*, would also cover the situation where an authorized user obtains the report under the guise of a business need and commences to use it improperly. No other section of the Act addresses itself to this problem, but it would seem to fall within the purview of the section. However, one further problem was left unsolved: what are the permissible uses of the report by the subscriber once he has used the report for legitimate business needs? Most likely, the applicable law on libel or slander would apply because the immunity of qualified privilege would not attach to a user in a case such as this.

[163]15 U.S.C. § 1681s (1970).

[164]Interview with Ms. Goodman, *supra* note 36.

[165]There may have been a small amount of conflict of interest here because Congressman Patman had also introduced two successive bills. *See* note 40 *supra*.

[166]*See Hearings on S. 823*, *supra* note 42.

of the testimony repeated earlier statements by many of the same witnesses who had appeared before other committees. Although these hearings have been generally criticized,[167] they served a very useful purpose—they caused public and political attention to be focused upon the documented abuse. This was the primary purpose of the Proxmire hearings.[168] Nothing new by way of information was heard which was not already known. The effort was to publicize the fact that the efforts within this area being made by Congress were serious both as a warning to the credit industry and as encouragement to consumers and constituents.

During the months that followed, the committee digested the information and recommendations, and, on October 9, 1969, S. 823 was reported out of executive committee. The full committee then met on October 22 and ordered the bill reported with the amendments made by the committee.[169] The bill was passed as reported on November 5 with little debate by a voice vote of the Senate,[170] and, on November 12 the House referred it to the House Committee on Banking and Currency, where it was to be stalled for many months.

One of the possible reasons for the apparent lethargy of the House Committee was its self-interest in holding hearings on an alternate bill submitted by Congresswoman Leonore Sullivan which she had titled the "Good Name Protection Bill."[171] In general the House bill provided more stringent controls on the credit agencies and possibly greater protection for the consumer as a result. Seven days of hearings were held during the middle and latter part of March and the early part of April 1970.[172] Again, the hearings did little more than repeat previous performances. However, the hearings did provide a forum for a comparative analysis of the merits and shortcomings of both H.R. 16340 and S. 823.[173] The bill was then sent to the committee which never reported it out. Three days of closed executive sessions were held, but at no time was a quorum present.[174] Consequently, H.R. 16340 died a quiet death. Its influence remained, however. During the mid-summer

---

[167] *See* note 62 *supra* and accompanying text.

[168] Interview with Mr. Kenneth McLean, *supra* note 141.

[169] S. REP. No. 517, 91st Cong. 1st Sess., (1969). One author wrote that the Committee had, in effect, emasculated the bill. *See* Miller, *Detour to 1984*, NATION, June 1, 1970, at 669. This author, however, disagrees, based on the analysis above.

[170] 27 CONGRESSIONAL QUARTERLY 2257 (November 14, 1969) (Weekly Report).

[171] H.R. 16340, 91st Cong., 2d Sess. (1969).

[172] *See Hearings on H.R. 16340 Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 2d Sess. (1970). *See also* 28 CONGRESSIONAL QUARTERLY 1017-18 (April 17, 1970) (Weekly Report).

[173] *See* 26 CONGRESSIONAL QUARTERLY ALMANAC 625 (1970).

[174] Interview with Mr. Charles Witter, *supra* note 33.

months, Mr. Kenneth McLean, the staff economist of the Senate Committee on Banking and Currency who had helped Proxmire draft S. 823, drafted five separate rewrites of S. 823 incorporating some of the provisions of H.R. 16340, most notably those sections dealing with disclosure and civil liability.[175]

During the Sullivan hearings, the House was engaged in another activity which was to be a major factor in the passage of the Fair Credit Reporting Act. On March 28, 1970, the House Committee on Banking and Currency reported out H.R. 15073, which was a bill to stop the practice of depositing funds secretly in Swiss banks, a tactic used by some to avoid taxes.[176] On May 25 the House passed H.R. 15073, and the bill was sent to the Senate.[177] Proxmire then added to this bill as non-germane amendments S. 721, his bill to regulate unsolicited credit cards, and S. 823, his Fair Credit Reporting Bill. The Senate passed H.R. 15073, as amended, in September and from there it went to the Conference Committee.[178]

The conferees agreed on a number of changes in the provisions of S. 823. The conference version required all reporting credit information—not just investigating agencies as in the Senate bill—to follow reasonable procedures to assure accuracy of their information. The conference agreement required any user of a report who rejected a consumer for credit, insurance, or employment to inform the consumer of the source of the report. The Senate version required the consumer to request the identification of the source in writing.[179] The Senate by voice vote agreed to the conference report on October 9, 1970, and the House adopted it, also by voice vote, on October 13, the final day of the session.[180] The Fair Credit Reporting Act was signed into law by the President on October 26, 1970.[181]

Conclusion

The Fair Credit Reporting Act does much toward providing the consumer with adequate protection from the abuses documented in the many congressional hearings. The Act provides specific regulation of obsolete information

---

[175]Interview with Mr. Kenneth McLean, *supra* note 141.

[176]H.R. REP. NO. 975, 91st Cong., 2d Sess. (1970). *See also* 26 CONGRESSIONAL QUARTERLY ALMANAC 884-89 (1970).

[177]*Id.* at 624.

[178]*Id.* at 626.

[179]*Id.*

[180]*Id.*

[181]The Act did not become effective, however, until April 25, 1971. A recent case has held that the FCRA was not to be given retroactive application. Wilson v. Retail Credit Co., 457 F.2d 1406 (5th Cir. 1972).

(§ 1681c), public record information (§ 1681k), and investigative consumer reports (§ 1681*l*) in addition to those abuses mentioned earlier. Yet the Act has come under attack because it does not provide enough protection.[182] The major criticism deals with the apparent ambiguity of the sections regulating access to the information and the sources. Section 1681g, detailing disclosure to the consumer, does not specifically allow for the consumer actually to inspect his record or to copy it, and this limitation has been utilized by the credit agencies.[183] It is theoretically possible that some information could be withheld at the time of disclosure to the consumer—a fact of which the consumer would never be aware unless he could actually inspect the report.

Another defect in the Act is that, although penalties are provided for unauthorized disclosure and access, there is no way for the consumer to know if this regulation has been violated because no record is required to be kept of those to whom the file has been distributed. Only in the case where such disclosure directly affects him in a negative way would the consumer be aware of a violation, and even then it is uncertain whether he would be able to discover the source.

A further criticism is that consumers cannot learn the source of gossip except in a civil suit.[184] The immediate response on the part of the credit agency is that divulging such sources would be tantamount to drying them up. It is necessary, argues the agency, that the source feel free to express his observations and opinions without the threat of a lawsuit hanging over his every word. Besides, by disclosing these sources, the agency would be a party to creating strife and bad feelings. As moralistic as these arguments may be, the ultimate effect of such anonymity is to permit the possibility of protected libel. If a person knows that he can say to an investigator with impunity something that under any other condition would be libelous, then there is a strong possibility he may say it. Accountability is the considered factor. Since value judgments and moral opinions of another's character have no criteria for quantitative or qualitative analysis, the possibility of

---

[182]*See generally* Nader, *The Dossier Invades the Home*, SATURDAY REV., April 17, 1971 at 18; Schrag, *Dossier Dictatorship*, SATURDAY REV., April 17, 1971 at 24; Note, *Protecting The Subjects of Credit Reports*, 80 YALE L.J. 1035 (1971). *See also* Note, *The Fair Credit Reporting Act*, 56 MINN. L. REV. 819 (1972); Note, *Protecting Privacy in Credit Reporting*, 24 STAN. L. REV. 550 (1972); Note, *Consumer Protection: Regulation and Liability of the Credit Reporting Industry*, 47 NOTRE DAME LAW. 1291 (1972); Comment, *The Fair Credit Reporting Act*, 23 ME. L. REV. 253 (1971).

[183]Interview with Mr. Keating, Manager, Retail Credit Co., Washington, D.C., on March 22, 1972.

[184]15 U.S.C. 1681g (2) (1970). The section states that the sources shall be available to the consumer under appropriate discovery procedures in the court in which the action is brought.

misinterpretation by any user is too great to allow anonymity. The adage "truth is its own defense" is very apropos to such a situation.

These shortcomings and others are not beyond remedy. Senator Proxmire plans to conduct further hearings in 1973 in order to evaluate the effect of the FCRA.[185] Should further legislation be necessary, given Proxmire's history of consumer concern, it will probably be forthcoming. However, it remains to be seen how the courts will interpret the sections of the Act which many feel are ambiguous.[186]

Since the passage of the Act, there has been scant litigation. In addition to a class action, filed in a Missouri federal district court but not yet litigated,[187] courts have interpreted the Act not to require the seizure of records of credit bureaus,[188] defined "consumer report" to exclude the report issued pursuant to a request for insurance for business purposes,[189] and found no

---

[185]Interview with Mr. Kenneth McLean, *supra* note 141.

[186]A possible alternative source of interpretation and application is the Federal Trade Commission which is primarily responsible for the administration of the Act. 15 U.S.C. § 1681s(a) (1970). A violation of the FCRA is an unfair trade practice under section 5(a) of the FTC Act. *Id.* However, the FTC has no substantive rulemaking authority. Therefore, it can only issue Advisory Opinions although it may enforce sanctions against violations of the Act as interpreted by those Opinions. National Petroleum Refiners Ass'n v. FTC, 340 F. Supp. 1343 (D.D.C. 1972). These Opinions are issued either through "the Commission's view" as published in the *Federal Register*, FTC Procedures and Rules of Practice, Subpart H, § 1.73, 36 Fed. Reg. 9294 (1971), or through staff interpretations which may be in response to individual requests. These are "informal staff opinions" rather than "the Commission's view", but there is no real practical difference. *Id.* at § 1.72.

[187]Millstone v. National Inspection Bureau (O'Hanlon Reports), Civil No. ____ (E.D. Mo. filed April 11, 1972). In this class action it is alleged that much of the information assembled by O'Hanlon Reports for Firemen's Fund American Insurance Co. was malicious neighborhood gossip and totally untrue. It seeks a court order barring O'Hanlon from disseminating the information, requiring the firm to make full disclosure of its files to consumers under investigation, and ordering the firm to revise its investigating techniques with regard to "accuracy, confidentiality and relevancy." In addition to injunctive relief, $2500 in actual damages and $100,000 in punitive damages are sought.

The report submitted on Mr. Millstone said that he was a drug user, he participated in many Washington demonstrations, he was a "hippie" type person who once wore a beard and had hair down to his shoulders, his children were completely undisciplined and damaged the neighbors' yards by frequently playing ball in them, he had been evicted from three previous residences, and that he was utterly lacking in reasoning and judgment.

Mr. Millstone is an editor of the St. Louis Post-Dispatch and covered the Supreme Court for the paper's Washington bureau until last August 1971.

[188]*See* Sauke v. FTC, 333 F. Supp. 1197 (N.D. Ga. 1971). The court also stated that the enforcement powers of the FTC are discretionary and applicable only in cases of public interest.

[189]Fernandez v. Retail Credit Co., 349 F. Supp. 652 (E.D. La. 1972), held that the scope of the Act as it relates to reports used to establish eligibility for insurance for personal, family, or household purposes cannot be extended to the establishment of eligibility for insurance for business purposes.

violation of the Act in the introduction of testimony of private investigators in Workman's Compensation Act proceedings.[190] Any trend will not become clear, however, for some time because cases of first impression are generally argued to the highest court which is often a matter of years.

One last point remains to be made concerning the legislative process itself as it has been reflected in the history of this Act. Nearly three years elapsed between the time Zablocki first brought the issue to the attention of Congress and when the Act became effective. Obviously, no one proposes that Congress enact legislation without having given anything less than full deliberation to the proposed legislation. Such deliberation must include complete investigation, an evaluation of alternatives, and consideration of the effects the legislation may have. Yet, as can be seen from the history of the FCRA, there was much repetition, much concern about political visibility, and much too much delay. Perhaps this is the price to be paid for the benefits received from uniform regulation through congressional mandate. For the consumer, the act was long overdue. Yet, in the long run, the legislative wait may be the only way we have to correct the ills of society—a society which is developing faster than its justice. As Professor Miller wrote:

> Continued vigilance and meaningful legislation are necessary to illuminate the road to the 21st century and reduce the likelihood of a detour to 1984.[191]

---

[190]*See* Soto v. Industrial Comm'n, 18 Ariz. App. 53, 500 P.2d 313 (1972). The court found no violation of the Act in this case, saying that the FCRA has no relevance to the question of admissibility of evidence in a compensation proceeding.

[191]Miller, *Detour to 1984*, NATION, June 1, 1970, at 669.

STATUTES AND DECISIONS

ADMINISTRATIVE PROCEDURE ACT (5 U.S.C. 500–559)

CHAPTER 5.—ADMINISTRATIVE PROCEDURE

SUBCHAPTER I.—GENERAL PROVISIONS

Sec.
500. Administrative practice; general provisions.
501. Advertising practice; restrictions.
502. Administrative practice; Reserves and National Guardsmen.
503. Witness fees and allowances.

SUBCHAPTER II.—ADMINISTRATIVE PROCEDURE

551. Definitions.
552. Public information; agency rules, opinions, orders, records, and proceedings.
553. Rule making.
554. Adjudications.
555. Ancillary matters.
556. Hearings; presiding employees; powers and duties; burden of proof; evidence; record as basis of decision.
557. Initial decisions, conclusiveness; review by agency; submissions by parties; contents of decisions; record.
558. Imposition of sanctions; determination of applications for licenses; suspension, revocation, and expiration of licenses.
559. Effect on other laws; effect of subsequent statute.

AMENDMENTS

1967—Pub. L. 90–98, § 1(1)(B), Sept. 11, 1967, 81 Stat. 195, added item 500.
Pub. L. 90–23, § 2, June 5, 1967, 81 Stat. 56, substituted "Public information; agency rules, opinions, orders, records and proceedings" for "Publication of information, rules, opinions, orders, and public records" in item 552.

SUBCHAPTER I.—GENERAL PROVISIONS

§ 500. Administrative practice; general provisions.

(a) For the purpose of this section—
(1) "agency" has the meaning given it by section 551 of this title; and
(2) "State" means a State, a territory or possession of the United States including a Commonwealth, or the District of Columbia.

(b) An individual who is a member in good standing of the bar of the highest court of a State may represent a person before an agency on filing with the agency a written declaration that he is currently qualified as provided by this subsection and is authorized to represent the particular person in whose behalf he acts.

(c) An individual who is duly qualified to practice as a certified public accountant in a State may represent a person before the Internal Revenue Service of the Treasury Department on filing with that agency a written declaration that he is currently qualified as provided by this subsection and is authorized to represent the particular person in whose behalf he acts.

(d) This section does not—
(1) grant or deny to any individual who is not qualified as provided by subsection (b) or (c) of this section the right to appear for or represent a person before an agency or in an agency proceeding;
(2) authorize or limit the discipline, including disbarment, of individuals who appear in a representative capacity before an agency;

(3) authorize an individual who is a former employee of an agency to represent a person before an agency when the representation is prohibited by statute or regulation; or

(4) prevent an agency from requiring a power of attorney as a condition to the settlement of a controversy involving the payment of money.

(e) Subsections (b)–(d) of this section do not apply to practice before the Patent Office with respect to patent matters that continue to be covered by chapter 3 (sections 31–33) of title 35.

(f) When a participant in a matter before an agency is represented by an individual qualified under subsection (b) or (c) of this section, a notice or other written communication required or permitted to be given the participant in the matter shall be gven to the representative in addition to any other service specifically required by statute. When a participant is represented by more than one such qualified representative, service on any one of the representatives is sufficient. (Added Pub. L. 90–83, § 1(1)(A), Sept. 11, 1967, 81 Stat. 195.)

§ 501. Advertising practice; restrictions.

An individual, firm, or corporation practicing before an agency of the United States may not use the name of a Member of either House of Congress or of an individual in the service of the United States in advertising the business. (Pub. L. 89–554, Sept. 6, 1966, 89 Stat. 381.)

§ 502. Administrative practice; Reserves and National Guardsmen.

Membership in a reserve component of the armed forces or in the National Guard does not prevent an individual from practicing his civilian profession or occupation before, or in connection with, an agency of the United States. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 381.)

§ 503. Witness fees and allowances.

(a) For the purpose of this section, "agency" has the meaning given it by section 5721 of this title.

(b) A witness is entitled to the fees and allowances allowed by statute for witnesses in the courts of the United States when—

(1) he is subpenaed under section 304(a) of this title; or

(2) he is subpenaed to and appears at a hearing before an agency authorized by law to hold hearings and subpena witnesses to attend the hearings.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 381.)

SUBCHAPTER II.—ADMINISTRATIVE PROCEDURE

Popular Name

The provisions of this subchapter and chapter 7 of this title were originally enacted by act June 11, 1946, ch. 324, 60 Stat. 237, popularly known as the "Administrative Procedure Act". That Act was repealed as part of the general revision of this title by Pub. L. 89–554 and its provisions incorporated into this subchapter and chapter 7 hereof.

§ 551. Definitions.

For the purpose of this subchapter—

(1) "agency" means each authority of the Government of the United States, whether or not it is within or subject to review by another agency, but does not include—

(A) the Congress;

(B) the courts of the United States;

(C) the governments of the territories or possessions of the United States;

(D) the government of the District of Columbia;

or except as to the requirements of section 552 of this title—

(E) agencies composed of representatives of the parties or of representatives of organizations of the parties to the disputes determined by them;

(F) courts martial and military commissions;

(G) military authority exercised in the field in time of war or in occupied territory; or

(H) functions conferred by sections 1738, 1739, 1743, and 1744 of title 12; chapter 2 of title 41; or sections 1622, 1884, 1891–1902, and former section 1641(b)(2), of title 50, appendix;

(2) "person" includes an individual, partnership, corporation, association, or public or private organization other than an agency;

(3) "party" includes a person or agency named or admitted as a party, or properly seeking and entitled as of right to be admitted as a party, in an agency proceeding, and a person or agency admitted by an agency as a party for limited purposes;

(4) "rule" means the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate of financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing;

(5) "rule making" means agency process for formulating, amending, or repealing a rule;

(6) "order" means the whole or a part of a final disposition, whether affirmative, negative, injunctive, or declaratory in form, of an agency in a matter other than rule making but including licensing;

(7) "adjudication" means agency process for the formulation of an order;

(8) "license" includes the whole or a part of an agency permit, certificate, approval, registration, charter, membership, statutory exemption or other form of permission;

(9) "licensing" includes agency process respecting the grant, renewal, denial, revocation, suspension, annulment, withdrawal, limitation, amendment, modification; or conditioning of a license;

(10) "Sanction" includes the whole or a part of an agency—

(A) prohibition, requirement, limitation, or other condition affecting the freedom of a person;

(B) withholding of relief;

(C) imposition of penalty or fine;

(D) destruction, taking, seizure, or withholding of property;

(E) assessment of damages, reimbursement, restitution, compensation, costs, charges, or fees;

(F) requirement, revocation, or suspension of a license; or

(G) taking other compulsory or restrictive action;

(11) "relief" includes the whole or a part of an agency—

(A) grant of money, assistance, license, authority, exemption, exception, privilege, or remedy;

(B) recognition of a claim, right, immunity, privilege, exemption, or exception; or

(C) taking of other action on the application or petition of, and beneficial to, a person;

(12) "agency proceeding" means an agency process as defined by paragraphs (5), (7), and (9) of this section; and

(13) "agency action" includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 381.)

[FREEDOM OF INFORMATION ACT]

§ 552. Public information; agency rules, opinions, orders, records, and proceedings.

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public—

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying—

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; and

(C) administrative staff manuals and instructions to staff that affect a member of the public;

unless the materials are promptly published and copies offered for sale. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction. However, in each case the justification for the deletion shall be explained fully in writing. Each agency also shall maintain and make available for public inspection and copying a current index providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if—

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, on request for identifiable records made in accordance with published rules stating the time, place, fees to the extent authorized by statute, and procedure to be followed, shall make the records promptly available to any person. On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complaint. In such a case the court shall determine the matter de novo and the burden is on the agency to sustain its action. In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member. Except as to causes the court considers of greater importance, proceedings before the district court, as authorized by this paragraph, take precedence on the docket over all other causes and shall be assigned for hearing and trial at the earliest practicable date and expedited in every way.

(4) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(b) This section does not apply to matters that are—

(1) specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute;

37-583 O - 74 - pt. 2 - 13

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

(c) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 383; Pub. L. 90–23, § 1, June 5, 1967, 81 Stat. 54.)

§ 553. Rule making.

(a) This section applies, according to the provisions thereof, except to the extent that there is involved—

(1) a military or foreign affairs function of the United States; or

(2) a matter relating to agency management or personnel or to public property, loans, grants, benefits, or contracts.

(b) General notice of proposed rule making shall be published in the Federal Register, unless persons subject thereto are named and either personally served or otherwise have actual notice thereof in accordance with law. The notice shall include—

(1) a statement of the time, place, and nature of public rule making proceedings;

(2) reference to the legal authority under which the rule is proposed; and

(3) either the terms of substance of the proposed rule or a description of the subjects and issues involved.

Except when notice or hearing is required by statute, this subsection does not apply—

(A) to interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice; or

(B) when the agency for good cause finds (and incorporates the finding and a brief statement of reasons therefor in the rules issued) that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest.

(c) After notice required by this section, the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation. After consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose. When rules are required by statute to be made on the record after opportunity for an agency hearing, sections 556 and 557 of this title apply instead of this subsection.

(d) The required publication or service of a substantive rule shall be made not less than 30 days before its effective date, except—

(1) a substantive rule which grants or recognizes an exemption or relieves a restriction;

(2) interpetative rules and statements of policy; or

(3) as otherwise provided by the agency for good cause found and published with the rule.

(e) Each agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 383.)

§ 554. Adjudications.

(a) This section applies, according to the provisions thereof, in every case of adjudication required by statute to be determined on the record after opportunity for an agency hearing, except to the extent that there is involved—

(1) a matter subject to a subsequent trial of the law and the facts de novo in a court;

(2) the selection or tenure of an employee, except a hearing examiner appointed under section 3105 of this title;

(3) proceedings in which decisions rest solely on inspections, tests, or elections;

(4) the conduct of military or foreign affairs functions;

(5) cases in which an agency is acting as an agent for a court; or

(6) the certification of worker representatives.

(b) Persons entitled to notice of an agency hearing shall be timely informed of—

(1) the time, place, and nature of the hearings;

(2) the legal authority and jurisdiction under which the hearing is to be held; and

(3) the matters of fact and law asserted.

When private persons are the moving parties, other parties to the proceeding shall give prompt notice of issues controverted in fact or law; and in other instances agencies may by rule require responsive pleading. In fixing the time and place for hearings, due regard shall be had for the convenience and necessity of the parties or their representatives.

(c) The agency shall give all interested parties opportunity for—

(1) the submission and consideration of facts, arguments, offers of settlement, or proposals of adjustment when time, the nature of the proceeding, and the public interest permit; and

(2) to the extent that the parties are unable so to determine a controversy by consent, hearing and decision on notice and in accordance with sections 556 and 557 of this title.

(d) The employee who presides at the reception of evidence pursuant to section 556 of this title shall make the recommended decision or intial decision required by section 557 of this title, unless he becomes unavailable to the agency. Except to the extent required for the disposition of ex parte matters as authorized by law, such an employee may not—

(1) consult a person or party on a fact in issue, unless on notice and opportunity for all parties to participate; or

(2) be responsible to or subject to the supervision or direction of an employee or agent engaged in the performance of investigative or prosecuting functions for an agency.

An employee or agent engaged in the performance of investigative or prosecuting functions for an agency in a case may not, in that or a factually related case, participate or advise in the decision, recommended decision, or agency review pursuant to section 557 of this title, except as witness or counsel in public proceedings. This subsection does not apply—

(A) in determining applications for initial licenses;

(B) to proceedings involving the validity or application of rates, facilities, or practices of public utilities or carriers; or

(C) to the agency or a member or members of the body comprising the agency.

(e) The agency, with like effect as in the case of other orders, and in its sound discretion, may issue a declaratory order to terminate a controversy or remove uncertainty. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 384.)

§ 555. Ancillary matters.

(a) This section applies, according to the provisions thereof, except as otherwise provided by this subchapter.

(b) A person compelled to appear in person before an agency or representative thereof is entitled to be accompanied, represented, and advised by counsel or, if permitted by the agency, by other qualified representative. A party is entitled to appear in person or by or with counsel or other duly qualified representative in an agency proceeding. So far as the orderly conduct of public business permits, an interested person may appear before an agency or its responsible employees for the presentation, adjustment, or determination of an issue, request, or controversy in a proceeding, whether interlocutory, summary, or otherwise, or in connection with an agency function. With due regard for the convenience and necessity of the parties or their representatives and within a reasonable time, each agency shall proceed to conclude a matter presented to it. This subsection does not grant or deny a person who is not a lawyer the right to appear for or represent others before an agency or in an agency proceeding.

(c) Process, requirement of a report, inspection, or other investigative act or demand may not be issued, made, or enforced except as authorized by law. A person compelled to submit data or evidence is entitled to retain or, on payment of lawfully prescribed costs, procure a copy or transcript thereof, except that in a nonpublic investigatory proceeding the witness may for good cause be limited to inspection of the official transcript of his testimony.

(d) Agency subpenas authorized by law shall be issued to a party on request and, when required by rules of procedure, on a statement or showing of general relevance and reasonable scope of the evidence sought. On contest, the court shall sustain the subpena or similar process or demand to the extent that it is found to be in accordance with law. In a proceeding for enforcement, the court shall issue an order requiring the appearance of the witness or the production of the evidence or data within a reasonable time under penalty of punishment for contempt in case of contumacious failure to comply.

(e) Prompt notice shall be given of the denial in whole or in part of a written application, petition, or other request of an interested person made in connection with any agency proceedings. Except in affirming a prior denial or when the denial is self-explanatory, the notice shall be accompanied by a brief statement of the grounds for denial. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 385.)

§ 556. Hearings; presiding employees; powers and duties; burden of proof; evidence; record as basis of decision.

(a) This section applies, according to the provisions thereof, to hearings required by section 553 or 554 of this title to be conducted in accordance with this section.

(b) There shall preside at the taking of evidence—

(1) the agency;

(2) one or more members of the body which comprises the agency; or

(3) one or more hearing examiners appointed under section 3105 of this title.

This subchapter does not supersede the conduct of specified classes of proceedings, in whole or in part, by or before boards or other employees specially provided for by or designated under statute. The functions of presiding employees and of employees participating in decisions in accordance with section 557 of this title shall be conducted in an impartial manner. A presiding or participating employee may at any time disqualify himself. On the filing in good faith of a timely and sufficient affidavit of personal bias or other disqualification of a presiding or participating employee, the agency shall determine the matter as a part of the record and decision in the case.

(c) Subject to published rules of the agency and within its powers, employees presiding at hearings may—

(1) administer oaths and affirmations;

(2) issue subpenas authorized by law;

(3) rule on offers of proof and receive relevant evidence;

(4) take depositions or have depositions taken when the ends of justice would be served;

(5) regulate the course of the hearing;

(6) hold conferences for the settlement or simplification of the issues by consent of the parties;

(7) dispose of procedural requests or similar matters;

(8) make or recommend decisions in accordance with section 557 of this title; and

(9) take other action authorized by agency rule consistent with this subchapter.

(d) Except as otherwise provided by statute, the proponent of a rule or order has the burden of proof. Any oral or documentary evidence may be received, but the agency as a matter of policy shall provide for the exclusion of irrelevant, immaterial, or unduly repetitious evidence. A sanction may not be imposed or rule or order issued except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence. A party is entitled to present his case or defense by oral or documentary evidence, to submit rebuttal evidence, and to conduct such cross-examination as may be required for a full and true disclosure of the facts. In rule making or determining claims for money or benefits or applications for initial licenses an agency may, when a party will not be prejudiced

thereby, adopt procedures for the submission of all or part of the evidence in written form.

(e) The transcript of testimony and exhibits, together with all papers and requests filed in the proceeding, constitutes the exclusive record for decision in accordance with section 557 of this title and, on payment of lawfully prescribed costs, shall be made available to the parties. When an agency decision rests on official notice of a material fact not appearing in the evidence in the record, a party is entitled, on timely request, to an opportunity to show the contrary. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 386.)

§ 557. Initial decisions; conclusiveness; review by agency; submissions by parties; contents of decisions; record.

(a) This section applies, according to the provisions thereof, when a hearing is required to be conducted in accordance with section 556 of this title.

(b) When the agency did not preside at the reception of the evidence, the presiding employee or, in cases not subject to section 554(d) of this title, an employee qualified to preside at hearings pursuant to section 556 of this title, shall initially decide the case unless the agency requires, either in specific cases or by general rule, the entire record to be certified to it for decision. When the presiding employee makes an initial decision, that decision then becomes the decision of the agency without further proceedings unless there is an appeal to, or review on motion of, the agency within time provided by rule. On appeal from or review of the initial decision, the agency has all the powers which it would have in making the initial decision except as it may limit the issues on notice or by rule. When the agency makes the decision without having presided at the reception of the evidence, the presiding employee or an employee qualified to preside at hearings pursuant to section 556 of this title shall first recommend a decision, except that in rule making or determining applications for initial licenses—

(1) instead thereof the agency may issue a tentative decision or one of its responsible employees may recommend a decision; or

(2) this procedure may be omitted in a case in which the agency finds on the record that due and timely execution of its functions imperatively and unavoidably so requires.

(c) Before a recommended, initial, or tentative decision, or a decision on agency review of the decision of subordinate employees, the parties are entitled to a reasonable oppportunity to submit for the consideration of the employees participating in the decisions—

(1) proposed findings and conclusions; or

(2) exceptions to the decisions or recommended decisions of subordinate employees or to tentative agency decisions; and

(3) supporting reasons for the exception or proposed findings or conclusions.

The record shall show the ruling on each finding, conclusion, or exception presented. All decisions, including initial, recommended, and tentative decisions, are a part of the record and shall include a statement of—

(A) findings and conclusions, and the reasons or basis therefor, on all the material issues of fact, law, or discretion presented on the record; and

(B) the appropriate rule, order, sanction, relief, or denial thereof.

§ 558. Imposition of sanctions; determination of applications for licenses; suspension, revocation, and expiration of licenses.

(a) This section applies, according to the provisions thereof, to the exercise of a power or authority.

(b) A sanction may not be imposed or a substantive rule or order issued except within jurisdiction delegated to the agency and as authorized by law.

(c) When application is made for a license required by law, the agency, with due regard for the rights and privileges of all the interested parties or adversely affected persons and within a reasonable time, shall set and complete proceedings required to be conducted in accordance with sections 556 and 557 of this title or other proceedings required by law and shall make its decision. Except in cases of willfulness or those in which public health, interest, or safety requires otherwise, the withdrawal, suspension, revocation, or annulment of a license is lawful only if, before the institution of agency proceedings therefor, the licensee has been given—

(1) notice by the agency in writing of the facts or conduct which may warrant the action; and

(2) opportunity to demonstrate or achieve compliance with all lawful requirements.

When the licensee has made timely and sufficient application for a renewal or a new license in accordance with agency rules, a license with reference to an activity of a continuing nature does not expire until the application has been finally determined by the agency. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 388.)

§ 559. Effect on other laws; effect of subsequent statute.

This subchapter, chapter 7, and sections 1305, 3105, 3344, 4301(2)(E), 5362, and 7521 of this title, and the provisions of section 5335(a)(B) of this title that relate to hearing examiners, do not limit or repeal additional requirements imposed by statute or otherwise recognized by law. Except as otherwise required by law, requirements or privileges relating to evidence or procedure apply equally to agencies and persons. Each agency is granted the authority necessary to comply with the requirements of this subchapter through the issuance of rules or otherwise. Subsequent statute may not be held to supersede or modify this subchapter, chapter 7, sections 1305, 3105, 3344, 4301(2)(E), 5362, or 7521 of this title, or the provisions of section 5335(a)(B) of this title that relate to hearing examiners, except to the extent that it does so expressly. (Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 388; Pub. L. 90–623, § 1(1), Oct. 22, 1968, 82 Stat. 1312.)

§ 757. Federal telecommunications fund

There is authorized to be established on the books of the Treasury, a Federal telecommunications fund, which shall be available without fiscal year limitation for expenses, including personal services, other costs, and the procurement by lease or purchase of equipment and operating facilities (including cryptographic devices) necessary for the operation of a Federal telecommunications system, to provide local and long distance voice, teletype, data, facsimile, and other communication services. There are authorized to be appropriated to said fund such sums as may be required which, together with the value, as determined by the Administrator, of supplies and equipment from time to time transferred to the Administrator under authority of section 486(f) of this title, less any liabilities assumed, shall constitute the capital of the fund: *Provided*, That said fund shall be credited with (1) advances and reimbursements from available appropriations and funds of any agency (including the General Services Administration), organization, or persons for telecommunication services rendered and facilities made available thereto, at rates determined by the Administrator to approximate the costs thereof met by the fund (including depreciation of equipment, provision for accrued leave, and where appropriate, for terminal liability charges and for amortization of installation costs, but excluding, in the determination of rates prior to the fiscal year 1966, such direct operating expenses as may be directly appropriated for, which expenses may be charged to the fund and covered by advances or reimbursements from such direct appropriations) and (2) refunds or recoveries resulting from operations of the fund, including the net proceeds of disposal of excess or surplus personal property and receipts from carriers and others for loss of or damage to property: *Provided further*, That following the close of each fiscal year any net income, after making provision for prior year losses, if any, shall be transferred to the Treasury of the United States as miscellaneous receipts.

June 30, 1949, c. 288, Title I, § 110, as added Oct. 23, 1962, Pub.L. 87–847, 76 Stat. 1117.

§ 759. Procurement, maintenance, operation and utilization of automatic data processing equipment—Authority of Administrator to coordinate and provide for purchase, lease and maintenance of equipment by Federal agencies

(a) The Administrator is authorized and directed to coordinate and provide for the economic and efficient purchase, lease, and maintenance of automatic data processing equipment by Federal agencies.

Procurement, maintenance and repair of equipment; transfer between agencies; joint utilization; establishment and operation of equipment pools and data processing centers; delegation of Administrator's authority

(b) (1) Automatic data processing equipment suitable for efficient and effective use by Federal agencies shall be provided by the Administrator through purchase, lease, transfer of equipment from other Federal agencies, or otherwise, and the Administrator is authorized and directed to provide by contract or otherwise for the maintenance and repair of such equipment. In carrying out his responsibilities under this section the Administrator is authorized to transfer automatic data processing equipment between Federal agencies, to provide for joint utilization of such equipment by two or more Federal agencies, and to establish and operate equipment pools and data processing centers for the use of two or more such agencies when necessary for its most efficient and effective utilization.

(2) The Administrator may delegate to one or more Federal agencies authority to operate automatic data processing equipment pools and automatic data processing centers, and to lease, purchase, or maintain individual automatic data processing systems or specific units of equipment, including such equipment used in automatic data processing pools and automatic data processing centers, when such action is determined by the Administrator to be necessary for the economy and efficiency of operations, or when such action is essential to national defense or national security. The Administrator may delegate to one or more Federal agencies authority to lease, purchase, or maintain automatic data processing equipment to the extent to which he determines such action to be necessary and desirable to allow for the orderly implementation of a program for the utilization of such equipment.

Automatic data processing fund; establishment; uses; report to Bureau of Budget and Congress

(c) There is hereby authorized to be established on the books of the Treasury an automatic data processing fund, which shall be available without fiscal year limitation for expenses, including personal services, other costs, and the procurement by lease, purchase, transfer, or otherwise of equipment, maintenance, and repair of such equipment by contract or otherwise, necessary for the efficient coordination, operation, utilization of such equipment by and for Federal agencies: *Provided*, That a report of equipment inventory, utilization, and acquisitions, together with an account of receipts, disbursements, and transfers to miscellaneous receipts, under this authorization shall be made annually in connection with the budget estimates to the Director of the Bureau of the Budget and to the Congress, and the inclusion in appropriation acts of provisions regulating the operation of the automatic data processing fund, or limiting the expenditures therefrom, is hereby authorized.

Capital of fund; credits; transfer of net income to Treasury

(d) There are authorized to be appropriated to said fund such sums as may be required which, together with the value, as determined by the Administrator, of supplies and equipment from time to time transferred to the Administrator, shall constitute the capital of the fund: *Provided*, That said fund shall be credited with (1) advances and reimbursements from available appropriations and funds of any agency (including the General Services Administration), organization, or contractor utilizing such equipment and services rendered them, at rates determined by the Administrator to approximate the costs thereof met by the fund (including depreciation of equipment, provision for accrued leave, and for amortization of installation costs, but excluding, in the determination of rates prior to the fiscal year 1967, such direct operating expenses as may be directly appropriated for, which expenses may be charged to the fund and covered by advances or reimbursements from such direct appropriations) and (2) refunds or recoveries resulting from operations of the fund, including the net proceeds of disposal of excess or surplus personal property and receipts from carriers and others for loss of or damage to property: *Provided further*, That following the close of each fiscal year any net income, after making provisions for prior year losses, if any, shall be transferred to the Treasury of the United States as miscellaneous receipts.

Inapplicability of other inconsistent provisions of law

(e) The proviso following paragraph (4) in section 481(a) of this title and the provisions of section 474 of this title shall have no application in the administration of this section. No other provision of this Act or any other Act which is inconsistent with the

provisions of this section shall be applicable in the administration of this section.

Scientific and technological advisory services by Secretary of Commerce; recommendations to President; research

(f) The Secretary of Commerce is authorized (1) to provide agencies, and the Administrator of General Services in the exercise of the authority delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, and (2) to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under provisions of this subsection.

Limitations on Authority of Administrator and Secretary of Commerce; notice and review of Administrator's determinations

(g) The authority conferred upon the Administrator and the Secretary of Commerce by this section shall be exercised subject to direction by the President and to fiscal and policy control exercised by the Bureau of the Budget. Authority so conferred upon the Administrator shall not be so construed as to impair or interfere with the determination by agencies of their individual automatic data processing equipment requirements, including the development of specifications for and the selection of the types and configurations of equipment needed. The Administrator shall not interfere with, or attempt to control in any way, the use made of automatic data processing equipment or components thereof by any agency. The Administrator shall provide adequate notice to all agencies and other users concerned with respect to each proposed determination specifically affecting them or the automatic data processing equipment or components used by them. In the absence of mutual agreement between the Administrator and the agency or user concerned, such proposed determinations shall be subject to review and decision by the Bureau of the Budget unless the President otherwise directs.

June 30, 1949, c. 288, Title I, § 111, as added Oct. 30, 1965, Pub.L. 89–306, 79 Stat. 1127.

Public Law 91-508
91st Congress, H. R. 15073
October 26, 1970

An Act

To amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Federal Deposit Insurance Act, amendments.

TITLE I—FINANCIAL RECORDKEEPING

Chapter		Sec.
1.	INSURED BANKS AND INSURED INSTITUTIONS	101
2.	OTHER FINANCIAL INSTITUTIONS	121

Chapter 1.—INSURED BANKS AND INSURED INSTITUTIONS

Sec.
101. Retention of records by insured banks.
102. Retention of records by insured institutions.

§ 101. Retention of records by insured banks

The Federal Deposit Insurance Act is amended (1) by redesignating sections 21 and 22 as 22 and 23, respectively, and (2) by inserting the following new section immediately after section 20:

64 Stat. 873. 12 USC 1811 note.

"SEC. 21. (a) (1) The Congress finds that adequate records maintained by insured banks have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings. The Congress further finds that microfilm or other reproductions and other records made by banks of checks, as well as records kept by banks of the identity of persons maintaining or authorized to act with respect to accounts therein, have been of particular value in this respect.

81 Stat. 610. 12 USC 1830, 1831.

84 STAT. 1114

84 STAT. 1115

"(2) It is the purpose of this section to require the maintenance of appropriate types of records by insured banks in the United States where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.

"(b) Where the Secretary of the Treasury (referred to in this section as the 'Secretary') determines that the maintenance of appropriate types of records and other evidence by insured banks has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, he shall prescribe regulations to carry out the purposes of this section.

"(c) Each insured bank shall maintain such records and other evidence, in such form as the Secretary shall require, of the identity of each person having an account in the United States with the bank and of each individual authorized to sign checks, make withdrawals, or otherwise act with respect to any such account. The Secretary may make such exemptions from any requirement otherwise imposed under this subsection as are consistent with the purposes of this section.

"(d) Each insured bank shall make, to the extent that the regulations of the Secretary so require—

"(1) a microfilm or other reproduction of each check, draft, or similar instrument drawn on it and presented to it for payment; and

"(2) a record of each check, draft, or similar instrument received by it for deposit or collection, together with an identification of the party for whose account it is to be deposited or collected, unless the bank has already made a record of the party's identity pursuant to subsection (c).

"(e) Whenever any individual engages (whether as principal, agent, or bailee) in any transaction with an insured bank which is required

to be reported or recorded under the Currency and Foreign Transactions Reporting Act, the bank shall require and retain such evidence of the identity of that individual as the Secretary may prescribe as appropriate under the circumstances.

Post, p. 1118.

"(f) In addition to or in lieu of the records and evidence otherwise referred to in this section, each insured bank shall maintain such records and evidence as the Secretary may prescribe to carry out the purposes of this section.

"(g) Any type of record or evidence required under this section shall be retained for such period as the Secretary may prescribe for the type in question. Any period so prescribed shall not exceed six years unless the Secretary determines, having regard for the purposes of this section, that a longer period is necessary in the case of a particular type of record or evidence.

Report to Congress.

"(h) The Secretary shall include in his annual report to the Congress information on his implementation of the authority conferred by this section and any similar authority with respect to recordkeeping or reporting requirements conferred by other provisions of law."

84 STAT. 1115

84 STAT. 1116

§ 102. Retention of records by insured institutions

48 Stat. 1255; 81 Stat. 611. 12 USC 1724-1730c.

Title IV of the National Housing Act is amended by adding at the end thereof the following new section:

"SEC. 411. The Secretary of the Treasury shall prescribe such regulations as may be appropriate to carry out, with respect to insured institutions, the purposes set forth in section 21 of the Federal Deposit Insurance Act with respect to insured banks."

Ante, p. 1114.

Chapter 2.—OTHER FINANCIAL INSTITUTIONS

Sec.
121. Congressional findings and purpose.
122. Authority of Secretary with respect to reports on ownership and control.
123. Authority of Secretary with respect to recordkeeping and procedures.
124. Injunctions.
125. Civil penalties.
126. Criminal penalty.
127. Additional criminal penalty in certain cases.
128. Compliance.
129. Administrative procedure.

§ 121. Congressional findings and purpose

(a) The Congress finds that certain records maintained by businesses engaged in the functions described in section 123(b) of this Act have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings. The Congress further finds that the power to require reports of changes in the ownership, control, and managements of types of financial institutions referred to in section 122 of this Act may be necessary for the same purpose.

(b) It is the purpose of this chapter to require the maintenance of appropriate types of records and the making of appropriate reports by such businesses in the United States where such records or reports have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.

§ 122. Authority of Secretary with respect to reports on ownership and control

Where the Secretary determines that the making of appropriate reports by uninsured banks or uninsured institutions of any type with respect to their ownership, control, and managements and any changes therein has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, he may by regulation require such banks or institutions to make such reports as he determines in respect of such ownership, control, and managements and changes therein.

§ 123. Authority of Secretary with respect to recordkeeping and procedures

(a) Where the Secretary determines that the maintenance of appropriate records and procedures by any uninsured bank or uninsured institution, or any person engaging in the business of carrying on in the United States any of the functions referred to in subsection (b) of this section, has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, he may by regulation require such bank, institution, or person— 84 STAT. 1116

(1) to require, retain, or maintain, with respect to its functions as an uninsured bank or uninsured institution or its functions referred to in subsection (b), any records or evidence of any type which the Secretary is authorized under section 21 of the Federal Deposit Insurance Act to require insured banks to require, retain, or maintain; and 84 STAT. 1117

Ante, p. 1114.

(2) to maintain procedures to assure compliance with requirements imposed under this chapter. For the purposes of any civil or criminal penalty, a separate violation of any requirement under this paragraph occurs with respect to each day and each separate office, branch, or place of business in which the violation occurs or continues.

(b) The authority of the Secretary under this section extends to any person engaging in the business of carrying on any of the following functions:

(1) Issuing or redeeming checks, money orders, travelers' checks, or similar instruments, except as an incident to the conduct of its own nonfinancial business.

(2) Transferring funds or credits domestically or internationally.

(3) Operating a currency exchange or otherwise dealing in foreign currencies or credits.

(4) Operating a credit card system.

(5) Performing such similar, related, or substitute functions for any of the foregoing or for banking as may be specified by the Secretary in regulations.

§ 124. Injunctions

Whenever it appears to the Secretary that any person has engaged, is engaged, or is about to engage in any acts or practices constituting a violation of any regulation under this chapter, he may in his discretion bring an action, in the proper district court of the United States or the proper United States court of any territory or other place subject to the jurisdiction of the United States, to enjoin such acts or practices, and upon a proper showing a permanent or temporary injunction or restraining order shall be granted without bond. Upon application of the Secretary, any such court may also issue mandatory injunctions commanding any person to comply with any regulation of the Secretary under this chapter.

§ 125. Civil penalties

(a) For each willful violation of any regulation under this chapter, the Secretary may assess upon any person to which the regulation applies, and, if such person is a partnership, corporation, or other entity, upon any partner, director, officer, or employee thereof who willfully participates in the violation, a civil penalty not exceeding $1,000.

(b) In the event of the failure of any person to pay any penalty assessed under this section, a civil action for the recovery thereof may, in the discretion of the Secretary, be brought in the name of the United States.

§ 126. Criminal penalty

Whoever willfully violates any regulation under this chapter shall be fined not more than $1,000 or imprisoned not more than one year, or both.

§ 127. Additional criminal penalty in certain cases

Whoever willfully violates any regulation under this chapter, section 21 of the Federal Deposit Insurance Act, or section 411 of the National Housing Act, where the violation is committed in furtherance of the commission of any violation of Federal law punishable by imprisonment for more than one year, shall be fined not more than $10,000 or imprisoned not more than five years, or both.

Ante, p. 1114.
Ante, p. 1116.

§ 128. Compliance

The Secretary shall have the responsibility to assure compliance with the requirements of this title and may delegate such responsibility to the appropriate bank supervisory agency, or other supervisory agency.

§ 129. Administrative procedure

The administrative procedure and judicial review provisions of subchapter II of chapter 5 and chapter 7 of title 5, United States Code, shall apply to all proceedings under this chapter, section 21 of the Federal Deposit Insurance Act, and section 411 of the National Housing Act.

80 Stat. 381.
5 USC 551-559, 701-706.

TITLE II—REPORTS OF CURRENCY AND FOREIGN TRANSACTIONS

Chapter	Sec.
1. General Provisions	201
2. Domestic Currency Transactions	221
3. Reports of Exports and Imports of Monetary Instruments	231
4. Foreign Transactions	241

Chapter 1.—GENERAL PROVISIONS

Sec.
201. Short title.
202. Purpose.
203. Definitions and rules of construction.
204. Regulations.
205. Compliance.
206. Exemptions.
207. Civil penalty.
208. Injunctions.
209. Criminal penalty.
210. Additional criminal penalty in certain cases.
211. Immunity of witnesses.
212. Availability of information to other Federal agencies.
213. Administrative procedure.

Citation of title.

§ 201. Short title

This title may be cited as the "Currency and Foreign Transactions Reporting Act".

§ 202. Purpose

It is the purpose of this title to require certain reports or records where such reports or records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.

§ 203. Definitions and rules of construction

(a) The definitions and rules of construction set forth in this section apply for the purposes of this title.

(b) The term "Secretary" means the Secretary of the Treasury.

(c) The term "person" includes natural persons, partnerships, trusts, estates, associations, corporations, and all entities cognizable

as legal personalities. The term also includes any governmental department or agency specified by the Secretary either for the purpose of this title generally or any particular requirement thereunder.

(d) The term "United States", used in a geographical sense, includes the States and the District of Columbia, and to the extent the Secretary shall by regulation specify, either for the purposes of this title generally or any particular requirement thereunder, the Commonwealth of Puerto Rico, the possessions of the United States, United States military establishments, and United States diplomatic establishments.

(e) The term "financial institution" means any person which does business in any one or more of the following capacities:

(1) an insured bank as defined in section 3 of the Federal Deposit Insurance Act; 64 Stat. 873. 12 USC 1813.

(2) a commercial bank or trust company;

(3) a private banker;

(4) an agency or a branch within the United States of any foreign bank;

(5) an insured institution as defined in section 401 of the National Housing Act; 48 Stat. 1255. 12 USC 1724.

(6) a savings bank, building and loan association, credit union, industrial bank, or other thrift institution;

(7) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934; 48 Stat. 881. 15 USC 78a.

(8) a broker or dealer in securities or commodities;

(9) an investment banker or investment company;

(10) a currency exchange;

(11) an issuer, redeemer or cashier of travelers' checks, checks, money orders, or similar instruments;

(12) an operator of a credit card system;

(13) an insurance company;

(14) a dealer in precious metals, stones, or jewels;

(15) a pawnbroker;

(16) a loan or finance company;

(17) a travel agency;

(18) a licensed transmitter of funds;

(19) a telegraph company;

(20) a Federal, State, or local government institution which performs any of the functions of any of the businesses listed above; or

(21) any other type of business or institution performing similar, related, or substitute functions specified by the Secretary by regulation for the purposes of the provision of this title to which the regulation relates.

(f) The term "domestic", used with reference to institutions or agencies, limits the applicability of the provision wherein it appears to the performance by such institutions or agencies of functions within the United States.

(g) The term "financial agency" means any person which acts in the capacity of a financial institution or in the capacity of a bailee, depository trustee, agent, or in any other similar capacity with respect to money, credit, securities, or gold or transactions therein, on behalf of any person other than a government, a monetary or financial authority when acting as such, or an international financial institution of which the United States is a member.

(h) The term "foreign", used with reference to institutions or agencies, limits the applicability of the provision wherein it appears to the performance by such institutions or agencies of functions outside the United States.

(i) References to this title or any provision thereof include regulations issued under this title or the provision thereof in question.

(j) All reports required under this title and all records of any such reports are specifically exempted from disclosure under section 552 of title 5, United States Code.

81 Stat. 54.

62 Stat. 749.

(k) For the purposes of section 1001 of title 18, United States Code, the contents of reports required under any provision of this title are statements and representations in matters within the jurisdiction of an agency of the United States.

(l) The term "monetary instruments" means coin and currency of the United States, and in addition, such foreign coin and currencies, and such types of travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, and stock with title passing upon delivery, or the equivalent thereof, as the Secretary may by regulation specify for the purposes of the provision of this title to which the regulation relates.

§ 204. Regulations

The Secretary shall prescribe such regulations as he may deem appropriate to carry out the purposes of this title.

§ 205. Compliance

(a) The Secretary shall have the responsibility to assure compliance with the requirements of this title and may delegate such responsibility to the appropriate bank supervisory agency, or other supervisory agency.

(b) The Secretary may by regulation require any class of domestic financial institutions to maintain such procedures as he may deem appropriate to assure compliance with the provisions of this title. For the purposes of both civil and criminal penalties for violations of this section, a separate violation shall be deemed to occur with respect to each day and each separate office, branch, or place of business in which the violation occurs or continues.

§ 206. Exemptions

The Secretary may make such exemptions from any requirement otherwise imposed under this title as he may deem appropriate. Any such exemption may be conditional or unconditional, by regulation, order, or licensing, or any combination thereof, and may relate to any particular transaction, to the type or amount of the transaction, to the party or parties or the classification of parties, or to any combination thereof. The Secretary may in his discretion, in any manner giving actual or constructive notice to the parties affected, revoke any exemption made under this section. Any such revocation shall remain in effect pending any judicial review.

§ 207. Civil penalty

(a) For each willful violation of this title, the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who willfully participates in the violation, a civil penalty not exceeding $1,000.

(b) In the event of the failure of any person to pay any penalty assessed under this title, a civil action for the recovery thereof may, in the discretion of the Secretary, be brought in the name of the United States.

§ 208. Injunctions

Whenever it appears to the Secretary that any person has engaged, is engaged, or is about to engage in any acts or practices constituting a violation of the provisions of this title, or of any order thereunder, he may in his discretion bring an action, in the proper district court

of the United States or the proper United States court of any territory or other place subject to the jurisdiction of the United States, to enjoin such acts or practices, and upon a proper showing a permanent or temporary injunction or restraining order shall be granted without bond. Upon application of the Secretary, any such court may also issue mandatory injunctions commanding any person to comply with the provisions of this title or any order of the Secretary made in pursuance thereof.

§ 209. Criminal penalty

Whoever willfully violates any provision of this title or any regulation under this title shall be fined not more than $1,000, or imprisoned not more than one year, or both.

§ 210. Additional criminal penalty in certain cases

Whoever willfully violates any provision of this title where the violation is—

(1) committed in furtherance of the commission of any other violation of Federal law, or

(2) committed as part of a pattern of illegal activity involving transactions exceeding $100,000 in any twelve-month period,

shall be fined not more than $500,000 or imprisoned not more than five years, or both.

§ 211. Immunity of witnesses

Whenever a witness refuses on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding involving any violation of this title before or ancillary to—

(1) a court or grand jury of the United States,

(2) an agency of the United States, or

(3) either House of Congress, a joint committee of the two Houses, or a committee or a subcommittee of either House,

and the person presiding over the proceeding communicates to the witness an order requiring him to give testimony or provide other information, the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination. No such testimony or other information so compelled under the order or evidence or other information which is obtained by the exploitation of such testimony may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order.

§ 212. Availability of information to other Federal agencies

The Secretary shall, upon such conditions and pursuant to such procedures as he may by regulation prescribe, make any information set forth in reports filed pursuant to this title available for a purpose consistent with the provisions of this title to any other department or agency of the Federal Government on the request of the head of such department or agency.

§ 213. Administrative procedure

Subject to section 203(j), the administrative procedure and judicial review provisions of subchapter II of chapter 5 and chapter 7 of title 5, United States Code, shall apply to all proceedings under this title.

Ante, p. 1118.

80 Stat. 381.
5 USC 551-559, 701-706.

Chapter 2.—DOMESTIC CURRENCY TRANSACTIONS

Sec.
221. Reports of currency transactions required.
222. Persons required to file reports.
223. Reporting procedure.

§ 221. Reports of currency transactions required

Transactions involving any domestic financial institution shall be reported to the Secretary at such time, in such manner, and in such detail as the Secretary may require if they involve the payment, receipt, or transfer of United States currency, or such other monetary instruments as the Secretary may specify, in such amounts, denominations, or both, or under such circumstances, as the Secretary shall by regulation prescribe.

§ 222. Persons required to file reports

The report of any transaction required to be reported under this chapter shall be signed or otherwise made both by the domestic financial institution involved and by one or more of the other parties thereto or participants therein, as the Secretary may require. If any party to or participant in the transaction is not an individual acting only for himself, the report shall identify the person or persons on whose behalf the transaction is entered into, and shall be made by the individuals acting as agents or bailees with respect thereto.

§ 223. Reporting procedure

(a) The Secretary may in his discretion designate domestic financial institutions, individually or by class, as agents of the United States to receive reports required under this chapter, except that an institution which is not insured, chartered, examined, or registered as such by any agency of the United States may not be so designated without its consent. The Secretary may suspend or revoke any such designation for any violation of this Act, or section 21 of the Federal Deposit Insurance Act, or section 411 of the National Housing Act.

Ante, pp. 1114, 1116.

(b) Any person (other than an institution designated under subsection (a)) required to file a report under this chapter with respect to a transaction with a domestic financial institution shall file the report with that institution, except that (1) if the institution is not designated under subsection (a), the report shall be filed as the Secretary shall prescribe, and (2) any such person may, at his election and in lieu of filing the report in the manner hereinabove prescribed, file the report with the Secretary. Domestic financial institutions designated under subsection (a) shall transmit reports filed with them, and shall file their own reports, as the Secretary shall prescribe.

Chapter 3.—REPORTS OF EXPORTS AND IMPORTS OF MONETARY INSTRUMENTS

Sec.
231. Reports required.
232. Forfeiture.
233. Civil liability.
234. Remission by the Secretary.
235. Enforcement authority.

§ 231. Reports required

(a) Except as provided in subsection (c) of this section, whoever, whether as principal, agent, or bailee, or by an agent or bailee, knowingly—

(1) transports or causes to be transported monetary instruments—

(A) from any place within the United States to or through any place outside the United States, or

(B) to any place within the United States from or through any place outside the United States, or

(2) receives monetary instruments at the termination of their transportation to the United States from or through any place outside the United States

in an amount exceeding $5,000 on any one occasion shall file a report or reports in accordance with subsection (b) of this section.

(b) Reports required under this section shall be filed at such times and places, and may contain such of the following information and any additional information, in such form and in such detail, as the Secretary may require:

(1) The legal capacity in which the person filing the report is acting with respect to the monetary instruments transported.

(2) The origin, destination, and route of the transportation.

(3) Where the monetary instruments are not legally and beneficially owned by the person transporting the same, or are transported for any purpose other than the use in his own behalf of the person transporting the same, the identities of the person from whom the monetary instruments are received, or to whom they are to be delivered, or both.

(4) The amounts and types of monetary instruments transported.

(c) Subsection (a) does not apply to any common carrier of passengers in respect of monetary instruments in the possession of its passengers, nor to any common carrier of goods in respect of shipments of monetary instruments not declared to be such by the shipper.

§ 232. Forfeiture

(a) Any monetary instruments which are in the process of any transportation with respect to which any report required to be filed under section 231(1) either has not been filed or contains material omissions or misstatements are subject to seizure and forfeiture to the United States.

(b) For the purpose of this section, monetary instruments transported by mail, by any common carrier, or by any messenger or bailee, are in process of transportation from the time they are delivered into the possession of the postal service, common carrier, messenger, or bailee until the time they are delivered into or retained in the possession of the addressee or intended recipient or any agent of the addressee or intended recipient for purposes other than further transportation within, or across any border of, the United States.

§ 233. Civil liability

The Secretary may assess a civil penalty upon any person who fails to file any report required under section 231, or who files such a report containing any material omission or misstatement. The amount of the penalty shall not exceed the amount of the monetary instruments with respect to whose transportation the report was required to be filed. The liabilities imposed by this chapter are in addition to any other liabilities, civil or criminal, except that the liability under this section shall be reduced by any amount actually forfeited under section 232.

§ 234. Remission by the Secretary

The Secretary may in his discretion remit any forfeiture or penalty under this chapter in whole or in part upon such terms and conditions as he deems reasonable and just.

§ 235. Enforcement authority

(a) If the Secretary has reason to believe that monetary instruments are in the process of transportation and with respect to which a report required under section 231 has not been filed or contains material omissions or misstatements, he may apply to any court of competent jurisdiction for a search warrant. Upon a showing of probable cause, the court may issue a warrant authorizing the search of any or all of the following: Search warrant.

(1) One or more designated persons.

(2) One or more designated or described places or premises.

(3) One or more designated or described letters, parcels, packages, or other physical objects.

(4) One or more designated or described vehicles.

Any application for a search warrant pursuant to this section shall be accompanied by allegations of fact supporting the application.

(b) This section is not in derogation of the authority of the Secretary under any other law.

Chapter 4.—FOREIGN TRANSACTIONS

Sec.
241. Records and reports required.
242. Classifications and requirements.

§ 241. Records and reports required

(a) The Secretary of the Treasury, having due regard for the need to avoid impeding or controlling the export or import of currency or other monetary instruments and having due regard also for the need to avoid burdening unreasonably persons who legitimately engage in transactions with foreign financial agencies, shall by regulation require any resident or citizen of the United States, or person in the United States and doing business therein, who engages in any transaction or maintains any relationship, directly or indirectly, on behalf of himself or another, with a foreign financial agency to maintain records or to file reports, or both, setting forth such of the following information, in such form and in such detail, as the Secretary may require:

(1) The identities and addresses of the parties to the transaction or relationship.

(2) The legal capacities in which the parties to the transaction or relationship are acting, and the identities of the real parties in interest if one or more of the parties are not acting solely as principals.

(3) A description of the transaction or relationship including the amounts of money, credit, or other property involved.

(b) No person required to maintain records under this section shall be required to produce or otherwise disclose the contents of the records except in compliance with a subpena or summons duly authorized and issued or as may otherwise be required by law.

§ 242. Classifications and requirements

The Secretary may prescribe:

(1) Any reasonable classification of persons subject to or exempt from any requirement imposed under section 241.

(2) The foreign country or countries as to which any requirement imposed under section 241 applies or does not apply if, in the judgment of the Secretary, uniform applicability of any such requirement to all foreign countries is unnecessary or undesirable.

(3) The magnitude of transactions subject to any requirement imposed under section 241.

(4) Types of transactions subject to or exempt from any requirement imposed under section 241.

(5) Such other matters as he may deem necessary to the application of this chapter.

TITLE III—MARGIN REQUIREMENTS

§ 301. Amendment of section 7 of the Securities Exchange Act of 1934

48 Stat. 886; 82 Stat. 452.

(a) Section 7 of the Securities Exchange Act of 1934 (15 U.S.C. 78g) is amended by adding at the end thereof the following new subsection:

"(f)(1) It is unlawful for any United States person, or any foreign person controlled by a United States person or acting on behalf of or in conjunction with such person, to obtain, receive, or enjoy the beneficial use of a loan or other extension of credit from any lender (without regard to whether the lender's office or place of business is in a State or the transaction occurred in whole or in part within a State) for the purpose of (A) purchasing or carrying United States securities, or (B) purchasing or carrying within the United States of any other securities, if, under this section or rules and regulations prescribed thereunder, the loan or other credit transaction is prohibited or would be prohibited if it had been made or the transaction had otherwise occured in a lender's office or other place of business in a State.

"(2) For the purposes of this subsection—

"(A) The term 'United States person' includes a person which is organized or exists under the laws of any State or, in the case of a natural person, a citizen or resident of the United States; a domestic estate; or a trust in which one or more of the foregoing persons has a cumulative direct or indirect beneficial interest in excess of 50 per centum of the value of the trust. "United States person."

"(B) The term 'United States security' means a security (other than an exempted security) issued by a person incorporated under the laws of any State, or whose principal place of business is within a State. "United States security."

"(C) The term 'foreign person controlled by a United States person' includes any noncorporate entity in which United States persons directly or indirectly have more than a 50 per centum beneficial interest, and any corporation in which one or more United States persons, directly or indirectly, own stock possessing more than 50 per centum of the total combined voting power of all classes of stock entitled to vote, or more than 50 per centum of the total value of shares of all classes of stock. "Foreign person controlled by a United States person."

"(3) The Board of Governors of the Federal Reserve System may, in its discretion and with due regard for the purposes of this section, by rule or regulation exempt any class of United States persons or foreign persons controlled by a United States person from the application of this subsection."

(b) The amendment made by subsection (a) of this section does not affect the continuing validity of any rule or regulation under section 7 of the Securities Exchange Act of 1934 in effect prior to the effective date of the amendment. Ante, p. 1124.

TITLE IV—EFFECTIVE DATES

§ 401. Effective dates

(a) Except as otherwise provided in this section, titles I, II, and III of this Act and the amendments made thereby take effect on the first day of the seventh calendar month which begins after the date of enactment. Ante, pp. 1114, 1118, 1124.

(b) The Secretary of the Treasury may by regulation provide that any provision of title I or II or any amendment made thereby shall be effective on any date not earlier than the publication of the regulation in the Federal Register and not later than the first day of the thirteenth calendar month which begins after the date of enactment. Publication in Federal Register.

(c) The Board of Governors of the Federal Reserve System may by regulation provide that the amendment made by title III shall be effective on any date not earlier than the publication of the regulation in the Federal Register and not later than the first day of the thirteenth calendar month which begins after the date of enactment. Publication in Federal Register.

TITLE V—PROVISIONS RELATING TO CREDIT CARDS

15 USC 1602.

SEC. 501. Section 103 of the Truth in Lending Act (82 Stat. 146) is amended by redesignating subsections (j), (k), and (l) as subsections (p), (q), and (r), respectively, and by adding after subsection (i) the following:

"Adequate notice." Infra.

"(j) The term 'adequate notice', as used in section 133, means a printed notice to a cardholder which sets forth the pertinent facts clearly and conspicuously so that a person against whom it is to operate could reasonably be expected to have noticed it and understood its meaning. Such notice may be given to a cardholder by printing the notice on any credit card, or on each periodic statement of account, issued to the cardholder, or by any other means reasonably assuring the receipt thereof by the cardholder.

"Credit card."

"(k) The term 'credit card' means any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit.

"Accepted credit card."

"(l) The term 'accepted credit card' means any credit card which the cardholder has requested and received or has signed or has used, or authorized another to use, for the purpose of obtaining money, property, labor, or services on credit.

"Cardholder."

"(m) The term 'cardholder' means any person to whom a credit card is issued or any person who has agreed with the card issuer to pay obligations arising from the issuance of a credit card to another person.

"Card issuer."

"(n) The term 'card issuer' means any person who issues a credit card, or the agent of such person with respect to such card.

"Unauthorized use."

"(o) The term 'unauthorized use', as used in section 133, means a use of a credit card by a person other than the cardholder who does not have actual, implied, or apparent authority for such use and from which the cardholder receives no benefit."

15 USC 1601 note. 15 USC 1641.

SEC. 502. (a) The Truth in Lending Act (82 Stat. 146) is amended by adding after section 131 the following sections:

"§ 132. Issuance of credit cards

Prohibition.

"No credit card shall be issued except in response to a request or application therefor. This prohibition does not apply to the issuance of a credit card in renewal of, or in substitution for, an accepted credit card.

"§ 133. Liability of holder of credit card

"(a) A cardholder shall be liable for the unauthorized use of a credit card only if the card is an accepted credit card, the liability is not in excess of $50, the card issuer gives adequate notice to the cardholder of the potential liability, the card issuer has provided the cardholder with a self-addressed, prestamped notification to be mailed by the cardholder in the event of the loss or theft of the credit card, and the unauthorized use occurs before the cardholder has notified the card issuer that an unauthorized use of the credit card has occurred or may occur as the result of loss, theft, or otherwise. Notwithstanding the foregoing, no cardholder shall be liable for the unauthorized use of any credit card which was issued on or after the effective date of this section, and, after the expiration of twelve months following such effective date, no cardholder shall be liable for the unauthorized use of any credit card regardless of the date of its issuance, unless (1) the conditions of liability specified in the preceding sentence are met, and (2) the card issuer has provided a method whereby the user of such card can be identified as the person authorized to use it. For the purposes of this section, a cardholder notifies a card issuer by taking such steps as may be reasonably required in the ordinary course of business to provide the card issuer with the pertinent information whether or not any particular officer, employee, or agent of the card issuer does in fact receive such information.

"(b) In any action by a card issuer to enforce liability for the use of a credit card, the burden of proof is upon the card issuer to show that the use was authorized or, if the use was unauthorized, then the burden of proof is upon the card issuer to show that the conditions of liability for the unauthorized use of a credit card, as set forth in subsection (a), have been met.

"(c) Nothing in this section imposes liability upon a cardholder for the unauthorized use of a credit card in excess of his liability for such use under other applicable law or under any agreement with the card issuer.

"(d) Except as provided in this section, a cardholder incurs no liability from the unauthorized use of a credit card.

"§ 134. Fraudulent use of credit card

Penalty.

"Whoever, in a transaction affecting interstate or foreign commerce, uses any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card to obtain goods or services, or both, having a retail value aggregating $5,000 or more, shall be fined not more than $10,000 or imprisoned not more than five years, or both."

(b) The table of contents of chapter 2 of the Truth in Lending Act is amended by adding at the end thereof the following:

82 Stat. 152.
15 USC 1631-1641.

"132. Issuance of credit cards.
"133. Liability of holder of credit card.
"134. Fraudulent use of credit card."

Effective dates.

SEC. 503. The amendments to the Truth in Lending Act made by this title become effective as follows:

(1) Section 132 of such Act takes effect upon the date of enactment of this title.

(2) Section 133 of such Act takes effect upon the expiration of 90 days after such date of enactment.

(3) Section 134 of such Act applies to offenses committed on or after such date of enactment.

TITLE VI—PROVISIONS RELATING TO CREDIT REPORTING AGENCIES

AMENDMENT OF CONSUMER CREDIT PROTECTION ACT

82 Stat. 146.
15 USC 1601 note.

SEC. 601. The Consumer Credit Protection Act is amended by adding at the end thereof the following new title:

"TITLE VI—CONSUMER CREDIT REPORTING

"Sec.
"601. Short title.
"602. Findings and purpose.
"603. Definitions and rules of construction.
"604. Permissible purposes of reports.
"605. Obsolete information.
"606. Disclosure of investigative consumer reports.
"607. Compliance procedures.
"608. Disclosures to governmental agencies.
"609. Disclosure to consumers.
"610. Conditions of disclosure to consumers.
"611. Procedure in case of disputed accuracy.
"612. Charges for certain disclosures.
"613. Public record information for employment purposes.
"614. Restrictions on investigative consumer reports.
"615. Requirements on users of consumer reports.
"616. Civil liability for willful noncompliance.
"617. Civil liability for negligent noncompliance.
"618. Jurisdiction of courts; limitation of actions.
"619. Obtaining information under false pretenses.
"620. Unauthorized disclosures by officers or employees.
"621. Administrative enforcement.
"622. Relation to State laws.

Citation of title.

"§ 601. Short title

"This title may be cited as the Fair Credit Reporting Act.

"§ 602. Findings and purpose

"(a) The Congress makes the following findings:

"(1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.

"(2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.

"(3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.

"(4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.

"(b) It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title.

"§ 603. Definitions and rules of construction

"(a) Definitions and rules of construction set forth in this section are applicable for the purposes of this title.

"(b) The term 'person' means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

"(c) The term 'consumer' means an individual.

"(d) The term 'consumer report' means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes, or (3) other purposes authorized under section 604. The term does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; or (C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under section 615.

Post, p. 1133.

"(e) The term 'investigative consumer report' means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such

items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

"(f) The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

"(g) The term 'file', when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

"(h) The term 'employment purposes' when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

"(i) The term 'medical information' means information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.

"§ 604. Permissible purposes of reports

"A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

"(1) In response to the order of a court having jurisdiction to issue such an order.

"(2) In accordance with the written instructions of the consumer to whom it relates.

"(3) To a person which it has reason to believe—

"(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

"(B) intends to use the information for employment purposes; or

"(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or

"(D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or

"(E) otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

"§ 605. Obsolete information

"(a) Except as authorized under subsection (b), no consumer reporting agency may make any consumer report containing any of the following items of information:

"(1) Bankruptcies which, from date of adjudication of the most recent bankruptcy, antedate the report by more than fourteen years.

"(2) Suits and judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period.

"(3) Paid tax liens which, from date of payment, antedate the report by more than seven years.

"(4) Accounts placed for collection or charged to profit and loss which antedate the report by more than seven years.

"(5) Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years.

"(6) Any other adverse item of information which antedates the report by more than seven years.

"(b) The provisions of subsection (a) are not applicable in the case of any consumer credit report to be used in connection with—

"(1) a credit transaction involving, or which may reasonably be expected to involve, a principal amount of $50,000 or more;

"(2) the underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of $50,000 or more; or

"(3) the employment of any individual at an annual salary which equals, or which may reasonably be expected to equal $20,000, or more.

"§ 606. Disclosure of investigative consumer reports

"(a) A person may not procure or cause to be prepared an investigative consumer report on any consumer unless—

"(1) it is clearly and accurately disclosed to the consumer that an investigative consumer report including information as to his character, general reputation, personal characteristics, and mode of living, whichever are applicable, may be made, and such disclosure (A) is made in a writing mailed, or otherwise delivered, to the consumer, not later than three days after the date on which the report was first requested, and (B) includes a statement informing the consumer of his right to request the additional disclosures provided for under subsection (b) of this section; or

"(2) the report is to be used for employment purposes for which the consumer has not specifically applied.

"(b) Any person who procures or causes to be prepared an investigative consumer report on any consumer shall, upon written request made by the consumer within a reasonable period of time after the receipt by him of the disclosure required by subsection (a)(1), shall make a complete and accurate disclosure of the nature and scope of the investigation requested. This disclosure shall be made in a writing mailed, or otherwise delivered, to the consumer not later than five days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the later.

"(c) No person may be held liable for any violation of subsection (a) or (b) of this section if he shows by a preponderance of the evidence that at the time of the violation he maintained reasonable procedures to assure compliance with subsection (a) or (b).

"§ 607. Compliance procedures

"(a) Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of section 605 and to limit the furnishing of consumer reports to the purposes listed under section 604. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 604.

"(b) Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.

"§ 608. Disclosures to governmental agencies

"Notwithstanding the provisions of section 604, a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency.

"§ 609. Disclosures to consumers

"(a) Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

"(1) The nature and substance of all information (except medical information) in its files on the consumer at the time of the request.

"(2) The sources of the information; except that the sources of information acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed: *Provided*, That in the event an action is brought under this title, such sources shall be available to the plaintiff under appropriate discovery procedures in the court in which the action is brought.

"(3) The recipients of any consumer report on the consumer which it has furnished—

"(A) for employment purposes within the two-year period preceding the request, and

"(B) for any other purpose within the six-month period preceding the request.

"(b) The requirements of subsection (a) respecting the disclosure of sources of information and the recipients of consumer reports do not apply to information received or consumer reports furnished prior to the effective date of this title except to the extent that the matter involved is contained in the files of the consumer reporting agency on that date.

"§ 610. Conditions of disclosure to consumers

"(a) A consumer reporting agency shall make the disclosures required under section 609 during normal business hours and on reasonable notice.

"(b) The disclosures required under section 609 shall be made to the consumer—

"(1) in person if he appears in person and furnishes proper identification; or

"(2) by telephone if he has made a written request, with proper identification, for telephone disclosure and the toll charge, if any, for the telephone call is prepaid by or charged directly to the consumer.

"(c) Any consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him pursuant to section 609.

"(d) The consumer shall be permitted to be accompanied by one other person of his choosing, who shall furnish reasonable identification. A consumer reporting agency may require the consumer to furnish a written statement granting permission to the consumer reporting agency to discuss the consumer's file in such person's presence.

"(e) Except as provided in sections 616 and 617, no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information

against any consumer reporting agency, any user of information, or any person who furnishes information to a consumer reporting agency, based on information disclosed pursuant to section 609, 610, or 615, except as to false information furnished with malice or willful intent to injure such consumer.

"§ 611. Procedure in case of disputed accuracy

"(a) If the completeness or accuracy of any item of information contained in his file is disputed by a consumer, and such dispute is directly conveyed to the consumer reporting agency by the consumer, the consumer reporting agency shall within a reasonable period of time reinvestigate and record the current status of that information unless it has reasonable grounds to believe that the dispute by the consumer is frivolous or irrelevant. If after such reinvestigation such information is found to be inaccurate or can no longer be verified, the consumer reporting agency shall promptly delete such information. The presence of contradictory information in the consumer's file does not in and of itself constitute reasonable grounds for believing the dispute is frivolous or irrelevant.

"(b) If the reinvestigation does not resolve the dispute, the consumer may file a brief statement setting forth the nature of the dispute. The consumer reporting agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute.

"(c) Whenever a statement of a dispute is filed, unless there is reasonable grounds to believe that it is frivolous or irrevelant, the consumer reporting agency shall, in any subsequent consumer report containing the information in question, clearly note that it is disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.

"(d) Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed information, the consumer reporting agency shall, at the request of the consumer, furnish notification that the item has been deleted or the statement, codification or summary pursuant to subsection (b) or (c) to any person specifically designated by the consumer who has within two years prior thereto received a consumer report for employment purposes, or within six months prior thereto received a consumer report for any other purpose, which contained the deleted or disputed information. The consumer reporting agency shall clearly and conspicuously disclose to the consumer his rights to make such a request. Such disclosure shall be made at or prior to the time the information is deleted or the consumer's statement regarding the disputed information is received.

"§ 612. Charges for certain disclosures

"A consumer reporting agency shall make all disclosures pursuant to section 609 and furnish all consumer reports pursuant to section 611(d) without charge to the consumer if, within thirty days after receipt by such consumer of a notification pursuant to section 615 or notification from a debt collection agency affiliated with such consumer reporting agency stating that the consumer's credit rating may be or has been adversely affected, the consumer makes a request under section 609 or 611(d). Otherwise, the consumer reporting agency may impose a reasonable charge on the consumer for making disclosure to such consumer pursuant to section 609, the charge for which shall be indicated to the consumer prior to making disclosure; and for furnishing notifications, statements, summaries, or codifications to person designated by the consumer pursuant to section 611(d), the charge for which shall be indicated to the consumer prior to furnish-

ing such information and shall not exceed the charge that the consumer reporting agency would impose on each designated recipient for a consumer report except that no charge may be made for notifying such persons of the deletion of information which is found to be inaccurate or which can no longer be verified.

"§ 613. Public record information for employment purposes

"A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall—

"(1) at the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or

"(2) maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date. For purposes of this paragraph, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported.

"§ 614. Restrictions on investigative consumer reports

"Whenever a consumer reporting agency prepares an investigative consumer report, no adverse information in the consumer report (other than information which is a matter of public record) may be included in a subsequent consumer report unless such adverse information has been verified in the process of making such subsequent consumer report, or the adverse information was received within the three-month period preceding the date the subsequent report is furnished.

"§ 615. Requirements on users of consumer reports

"(a) Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer is denied or the charge for such credit or insurance is increased either wholly or partly because of information contained in a consumer report from a consumer reporting agency, the user of the consumer report shall so advise the consumer against whom such adverse action has been taken and supply the name and address of the consumer reporting agency making the report.

"(b) Whenever credit for personal, family, or household purposes involving a consumer is denied or the charge for such credit is increased either wholly or partly because of information obtained from a person other than a consumer reporting agency bearing upon the consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, the user of such information shall, within a reasonable period of time, upon the consumer's written request for the reasons for such adverse action received within sixty days after learning of such adverse action, disclose the nature of the information to the consumer. The user of such information shall clearly and accurately disclose to the consumer his right to make such written request at the time such adverse action is communicated to the consumer.

"(c) No person shall be held liable for any violation of this section if he shows by a preponderance of the evidence that at the time of the alleged violation he maintained reasonable procedures to assure compliance with the provisions of subsections (a) and (b).

"§ 616. Civil liability for willful noncompliance

"Any consumer reporting agency or user of information which willfully fails to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of—

"(1) any actual damages sustained by the consumer as a result of the failure;

"(2) such amount of punitive damages as the court may allow; and

"(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

"§ 617. Civil liability for negligent noncompliance

"Any consumer reporting agency or user of information which is negligent in failing to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of—

"(1) any actual damages sustained by the consumer as a result of the failure;

"(2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

"§ 618. Jurisdiction of courts; limitation of actions

"An action to enforce any liability created under this title may be brought in any appropriate United States district court without regard to the amount in controversy, or in any other court of competent jurisdiction, within two years from the date on which the liability arises, except that where a defendant has materially and willfully misrepresented any information required under this title to be disclosed to an individual and the information so misrepresented is material to the establishment of the defendant's liability to that individual under this title, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

"§ 619. Obtaining information under false pretenses

"Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined not more than $5,000 or imprisoned not more than one year, or both.

"§ 620. Unauthorized disclosures by officers or employees

"Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined not more than $5,000 or imprisoned not more than one year, or both.

"§ 621. Administrative enforcement

"(a) Compliance with the requirements imposed under this title shall be enforced under the Federal Trade Commission Act by the Federal Trade Commission with respect to consumer reporting agencies and all other persons subject thereto, except to the extent that enforcement of the requirements imposed under this title is specifically committed to some other government agency under subsection (b) hereof. For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed

38 Stat. 717; 52 Stat. 114. 15 USC 58.

under this title shall constitute an unfair or deceptive act or practice in commerce in violation of section 5(a) of the Federal Trade Commission Act and shall be subject to enforcement by the Federal Trade Commission under section 5(b) thereof with respect to any consumer reporting agency or person subject to enforcement by the Federal Trade Commission pursuant to this subsection, irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act. The Federal Trade Commission shall have such procedural, investigative, and enforcement powers, including the power to issue procedural rules in enforcing compliance with the requirements imposed under this title and to require the filing of reports, the production of documents, and the appearance of witnesses as though the applicable terms and conditions of the Federal Trade Commission Act were part of this title. Any person violating any of the provisions of this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act as though the applicable terms and provisions thereof were part of this title.

66 Stat. 632.
15 USC 45.
52 Stat. 112.

"(b) Compliance with the requirements imposed under this title with respect to consumer reporting agencies and persons who use consumer reports from such agencies shall be enforced under—

"(1) section 8 of the Federal Deposit Insurance Act, in the case of:

64 Stat. 879; 80 Stat. 1046, 1054.

"(A) national banks, by the Comptroller of the Currency;

"(B) member banks of the Federal Reserve System (other than national banks), by the Federal Reserve Board; and

12 USC 1818.

"(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), by the Board of Directors of the Federal Deposit Insurance Corporation.

"(2) section 5(d) of the Home Owners Loan Act of 1933, section 407 of the National Housing Act, and sections 6(i) and 17 of the Federal Home Loan Bank Act, by the Federal Home Loan Bank Board (acting directly or through the Federal Savings and Loan Insurance Corporation), in the case of any institution subject to any of those provisions;

80 Stat. 1028.
12 USC 1464.
80 Stat. 1036.
12 USC 1730.
47 Stat. 727; 69 Stat. 640.
12 USC 1426, 1437.

"(3) the Federal Credit Union Act, by the Administrator of the National Credit Union Administration with respect to any Federal credit union;

73 Stat. 628; Ante, pp. 49, 994.

"(4) the Acts to regulate commerce, by the Interstate Commerce Commission with respect to any common carrier subject to those Acts;

12 USC 1751.
49 USC 1 et seq.

"(5) the Federal Aviation Act of 1958, by the Civil Aeronautics Board with respect to any air carrier or foreign air carrier subject to that Act; and

72 Stat. 731.
49 USC 1301 note.

"(6) the Packers and Stockyards Act, 1921 (except as provided in section 406 of that Act), by the Secretary of Agriculture with respect to any activities subject to that Act.

42 Stat. 159.
7 USC 181, 226, 227.

"(c) For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this title shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this title any other authority conferred on it by law.

"§ 622. Relation to State laws

"This title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to the collection, distribution, or use of any information on consumers, except to the extent that those laws are inconsistent with any provision of this title, and then only to the extent of the inconsistency."

EFFECTIVE DATE

82 Stat. 167.

SEC. 602. Section 504 of the Consumer Credit Protection Act is amended by adding at the end thereof the following new subsection:

"(d) Title VI takes effect upon the expiration of one hundred and eighty days following the date of its enactment."

Approved October 26, 1970.

LEGISLATIVE HISTORY:

HOUSE REPORTS: No. 91-975 (Comm. on Banking and Currency) and No. 91-1587 (Comm. of Conference).
SENATE REPORT No. 91-1139 accompanying S. 3678 (Comm. on Banking and Currency).
CONGRESSIONAL RECORD, Vol. 116 (1970):
May 25, considered and passed House.
Sept. 18, considered and passed Senate, amended.
Oct. 9, Senate agreed to conference report.
Oct. 13, House agreed to conference report.

CHAPTER 31—RECORDS MANAGEMENT BY FEDERAL AGENCIES

Sec.

3101. Records management by agency heads; general duties.
3102. Establishment of program of management.
3103. Storage, processing, and servicing of records.
3104. Certifications and determinations on transferred records.
3105. Safeguards.
3106. Unlawful removal, destruction of records.
3107. Authority of Comptroller General.

Cross References

Definitions applicable to provisions of Federal Property and Administrative Services Act of 1949, see section 472 of Title 40, Public Buildings, Property, and Works.

Definitions used in provisions respecting records management by Administrator of General Services to have same meaning when used in this chapter, see section 2901 of this title.

Exemptions from provisions of this chapter, see section 474 of Title 40, Public Buildings, Property, and Works.

Federal agency management program to provide for compliance with this chapter and regulations issued thereunder, see section 3102 of this title.

Federal Records Council, consultation of Administrator of General Services with Council with view of obtaining advice and assistance in carrying out the purposes of this chapter, see section 2701 of this title.

Final authority of Administrator in records practices under this chapter, see section 2910 of this title.

Legal status of reproductions made under regulations to carry out this chapter, see section 2112 of this title.

Reports from Federal agencies on their activities under this chapter, authority of Administrator of General Services to obtain; correction of violations, see section 2111 of this title.

§ 3101. Records management by agency heads; general duties

The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1297.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(a) (June 30, 1949, ch. 288, title V, § 506(a), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

37-583 O - 74 - pt. 2 - 15

§ 3102. Establishment of program of management

The head of each Federal agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. The program, among other things, shall provide for

(1) effective controls over the creation, maintenance, and use of records in the conduct of current business;

(2) cooperation with the Administrator of General Services in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value; and

(3) compliance with sections 2101–2113, 2501–2507, 2701, 2901, 2903–2909, and 3101–3107, of this title and the regulations issued under them.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(b) (June 30, 1949, ch. 288, title V, § 506(b), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3103. Storage, processing, and servicing of records

When the head of a Federal agency determines that it may effect substantial economies or increased operating efficiency, he shall provide for appropriate storage, processing, and servicing of records in a records center maintained and operated by the Administrator of General Services or, when approved by him, in a center maintained and operated by the head of the Federal agency.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964, ed., § 396(c) (June 30, 1949, ch. 288, title V, § 506(c), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3104. Certifications and determinations on transferred records

An official of the Government who is authorized to certify to facts on the basis of records in his custody, may certify to facts

on the basis of records that have been transferred by him or his predecessors to the Administrator of General Services, and may authorize the Administrator to certify to facts and to make administrative determinations on the basis of records transferred to the Administrator, notwithstanding any other law.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(d) (June 30, 1949, ch. 288, title V, § 506(d), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583, and amended Feb. 5, 1964, Pub.L. 88-265, 78 Stat. 8).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3105. Safeguards

The head of each Federal agency shall establish safeguards against the removal or loss of records he determines to be necessary and required by regulations of the Administrator of General Services. Safeguards shall include making it known to officials and employees of the agency—

(1) that records in the custody of the agency are not to be alienated or destroyed except in accordance with sections 3301–3314 of this title, and

(2) the penalties provided by law for the unlawful removal or destruction of records.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(e) (June 30, 1949, ch. 288, title V, § 506(e), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3106. Unlawful removal, destruction of records

The head of each Federal agency shall notify the Administrator of General Services of any actual, impending, or threatened unlawful removal, defacing, alteration, or destruction of records in the custody of the agency of which he is the head that shall come to his attention, and with the assistance of the Administrator shall initiate action through the Attorney General for the recovery of records he knows or has reason to believe have been unlawfully removed from his agency, or from another Federal agency whose records have been transferred to his legal custody.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(f) (June 30, 1949, ch. 288, title V, § 506(f), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

Cross References

Administrator of General Services authorized to transfer materials from private sources authorized to be received by him by this section, see section 2103 of this title.

Presidential archival depository: deposit of papers, documents, or other historical materials accepted under this section, see section 2108 of this title.

§ 3107. Authority of Comptroller General

Sections 2101–2113, 2501–2507, 2701, 2901, 2904–2910, and 3101–3107, of this title do not limit the authority of the Comptroller General of the United States with respect to prescribing accounting systems, forms, and procedures, or lessen the responsibility of collecting and disbursing officers for rendition of their accounts for settlement by the General Accounting Office.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1298.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., § 396(g) (June 30, 1949, ch. 288, title V, § 506(g), as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

CHAPTER 35—COORDINATION OF FEDERAL REPORTING SERVICES

Sec.

3501. Information for Federal agencies.
3502. Definitions.
3503. Duties of Director of the Bureau of the Budget.
3504. Designation of central collection agency.
3505. Independent collection by an agency prohibited.
3506. Determination of necessity for information; hearing.
3507. Cooperation of agencies in making information available.
3508. Unlawful disclosure of information; penalties; release of information to other agencies.
3509. Plans or forms for collecting information; submission to Director; approval.
3510. Rules and regulations.
3511. Penalty for failure to furnish information.

§ 3501. Information for Federal agencies

Information needed by Federal agencies shall be obtained with a minimum burden upon business enterprises, especially small business enterprises, and other persons required to furnish the information, and at a minimum cost to the Government. Unnecessary duplication of efforts in obtaining information through the use of reports, questionnaires, and other methods shall be eliminated as rapidly as practicable. Information collected and tabulated by a Federal agency shall, as far as is expedient, be tabulated in a manner to maximize the usefulness of the information to other Federal agencies and the public.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1302.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code 1964 ed., Supp. II, § 421 (Dec. 24, 1942, ch. 811, § 2, 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

Library References

Administrative Law and Procedure ⇐341 et seq.
Census ⇐1 et seq.
C.J.S. Census § 1 et seq.
C.J.S. Public Administrative Bodies and Procedure § 78 et seq.

§ 3502. Definitions

As used in this chapter—

"Federal agency" means an executive department, commission, independent establishment, corporation owned or controlled by the United States, board, bureau, division, service, office, authority, or administration in the executive branch of the Government; but does not include the General Accounting Office nor the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions;

"person" means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of persons, a State or territorial government or branch, or a political subdivision of a State or territory or a branch of a political subdivision;

"information" means facts obtained or solicited by the use of written report forms, application forms, schedules, questionnaires, or other similar methods calling either for answers to identical questions from ten or more persons other than agencies, instrumentalities, or employees of the United States or for answers to questions from agencies, instrumentalities, or employees of the United States which are to be used for statistical compilations of general public interest.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1302.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 426 (Dec. 24, 1942, ch. 811, § 7, 56 Stat. 1079).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

Cross References

Federal Register and Code of Federal Regulations, Federal agency defined, see section 1501 of this title.

§ 3503. Duties of Director of the Bureau of the Budget

With a view to carrying out the policy of this chapter, the Director of the Bureau of the Budget from time to time shall—

(1) investigate the needs of the various Federal agencies for information from business enterprises, from other persons, and from other Federal agencies;

(2) investigate the methods used by agencies in obtaining information; and

(3) coordinate as rapidly as possible the information-collecting services of all agencies with a view to reducing the cost to the Government of obtaining information and minimizing the burden upon business enterprises and other persons, and using, as far as practicable, for continuing organization, files of information and existing facilities of the established Federal agencies.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1303.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 422(a) (Dec. 24, 1942, ch. 811, § 3(a), 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3504. Designation of central collection agency

When, after investigation, the Director of the Bureau of the Budget is of the opinion that the needs of two or more Federal agencies for information from business enterprises and other persons will be adequately served by a single collecting agency, he shall fix a time and place for a hearing at which the agencies concerned and other interested persons may have an opportunity to present their views. After the hearing, the Director may issue an order designating a collecting agency to obtain information for two or more of the agencies concerned, and prescribing (with reference to the collection of information) the duties and functions of the collecting agency so designated and the Federal agencies for which it is to act as agent. The Director may modify the order from time to time as circumstances require, but modification may not be made except after investigation and hearing.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1303.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 422(b) (Dec. 24, 1942, ch. 811, § 3(b), 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3505. Independent collection by an agency prohibited

While an order or modified order is in effect, a Federal agency covered by it may not obtain for itself information which it is the duty of the collecting agency designated by the order to obtain.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1303.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 422(c) (Dec. 24, 1942, ch. 811, § 3(c), 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3506. Determination of necessity for information; hearing

Upon the request of a party having a substantial interest, or upon his own motion, the Director of the Bureau of the Budget may determine whether or not the collection of information by a Federal agency is necessary for the proper performance of the functions of the agency or for any other proper purpose. Before making a determination, he may give the agency and other interested persons an opportunity to be heard or to submit statements in writing. To the extent, if any, that the Director determines the collection of information by the agency is unnecessary, for any reason, the agency may not engage in the collection of the information.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1303.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 422(d) (Dec. 24, 1942, ch. 811, § 3(d), 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3507. Cooperation of agencies in making information available

For the purposes of this chapter, the Director of the Bureau of the Budget may require a Federal agency to make available to another Federal agency information obtained from any person after December 24, 1942, and all agencies are directed to cooperate to the fullest practicable extent at all times in making information available to other agencies.

This chapter does not apply to the obtaining or releasing of information by the Internal Revenue Service, the Comptroller of the Currency, the Bureau of the Public Debt, the Bureau of Accounts, and the Division of Foreign Funds Control of the Treasury Department, nor to the obtaining by a Federal bank supervisory agency of reports and information from banks as authorized by law and in the proper performance of the agency's functions in its supervisory capacity.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1304.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 422(e) (Dec. 24, 1942, ch. 811, § 3(e), 56 Stat. 1078).

Legislative History. For legislative history and purpose of Pub.L. 90–620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

Notes of Decisions

1. Commodity shipments

Under the provisions of this section, the Director of the Bureau of the Budget may require the Corps of Engineers, Department of the Army, to make available to the Maritime Commission information obtained since December 24, 1942, relating to commodities shipped in the domestic water trades of the United States, 1949, 41 Op.Atty.Gen., September 28.

§ 3508. Unlawful disclosure of information; penalties; release of information to other agencies

(a) If information obtained in confidence by a Federal agency is released by that agency to another Federal agency, all the provisions of law including penalties which relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information. The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

(b) Information obtained by a Federal agency from a person under this chapter may be released to another Federal agency only—

(1) in the form of statistical totals or summaries; or

(2) if the information as supplied by persons to a Federal agency had not, at the time of collection, been declared by that agency or by a superior authority to be confidential; or

(3) when the persons supplying the information consent to the release of it to a second agency by the agency to which the information was originally supplied; or

(4) when the Federal agency to which another Federal agency releases the information has authority to collect the information itself and the authority is supported by legal provision for criminal penalties against persons failing to supply the information.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1304.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 423 (Dec. 24, 1942, ch. 811, § 4, 56 Stat. 1079).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

Library References

Witnesses ⇐216.

C.J.S. Witnesses § 264.

Notes of Decisions

1. Authority for collection of information

Where the Director sought release of information from the Corps of Engineers to the Maritime Commission, the latter agency was entitled to such information on meeting the conditions that it had "authority to collect the information itself" and such authority was "supported by legal provision for criminal penalties." 1949, 41 Op.Atty.Gen., September 28.

§ 3509. Plans or forms for collecting information; submission to Director; approval

A Federal agency may not conduct or sponsor the collection of information upon identical items, from ten or more persons, other than Federal employees, unless, in advance of adoption or revision of any plans or forms to be used in the collection—

(1) the agency has submitted to the Director the plans or forms, together with copies of pertinent regulations and of other related materials as the Director of the Bureau of the Budget has specified; and

(2) the Director has stated that he does not disapprove the proposed collection of information.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1304.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 424 (Dec. 24, 1942, ch. 811, § 5, 56 Stat. 1079).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3510. Rules and regulations

The Director of the Bureau of the Budget may promulgate rules and regulations necessary to carry out sections 3501–3511 of this title.

Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1305.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 425 (Dec. 24, 1942, ch. 811, § 6, 56 Stat. 1079).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

§ 3511. Penalty for failure to furnish information

A person failing to furnish information required by an agency shall be subject to penalties specifically prescribed by law, and no other penalty may be imposed either by way of fine or imprisonment or by the withdrawal or denial of a right, privilege, priority, allotment, or immunity, except when the right, privilege, priority, allotment, or immunity is legally conditioned on facts which would be revealed by the information requested.

Pub.L. 90-620, Oct. 22, 1968, 82 Stat. 1305.

Historical and Revision Notes

Reviser's Note. Based on 44 U.S.Code, 1964 ed., Supp. II, § 427 (Dec. 24, 1942, ch. 811, § 8, 56 Stat. 1080).

Legislative History. For legislative history and purpose of Pub.L. 90-620, see 1968 U.S.Code Cong. and Adm.News, p. 4438.

tractor should seek the advice and recommendations of the National Historical Publications Commission. The Chairman of the Commission shall transmit to the Administrator from time to time, and at least annually, plans, estimates, and recommendations approved by the Commission.

(b) There is hereby authorized to be appropriated to the General Services Administration for the fiscal year ending June 30, 1973, and for each of the four succeeding fiscal years an amount not to exceed $2,000,000 for each year for the purposes specified in subsection (a) of this section: *Provided*, That such appropriations shall be available until exended when so provided in appropriation Acts.

As amended Pub.L. 92–546, § 1(c), Oct. 25, 1972, 86 Stat. 1155.

1972 Amendment. Pub.L. 92-546 designated existing provisions as subsec. (a) and added subsec. (b).

Authorization of Appropriations. Section 503(f) of Act June 30, 1949, c. 288, Title V, as added July 28, 1964, Pub.L. 88-383, 78 Stat. 335, and amended Aug. 8, 1968, Pub.L. 90-461, 82 Stat. 638 which authorized appropriation to the General Services Administration for the fiscal year ending June 30, 1965, and each of the nine succeeding fiscal years amount not exceeding $500,000 each year for the purposes of this section, was repealed by Pub.L. 92-546, § 2, Oct. 25, 1972, 86 Stat. 1155.

Legislative History. For legislative history and purpose of Pub.L. 92-546, see 1972 U.S.Code Cong. and Adm.News, p. 4462.

CHAPTER 29.—RECORDS MANAGEMENT BY ADMINISTRATOR OF GENERAL SERVICES

§ 2909. Retention of records

The Administrator of General Services may empower a Federal agency, upon the submission of evidence of need, to retain records for a longer period than that specified in disposal schedules; and, in accordance with regulations promulgated by him, may withdraw disposal authorizations covering records listed in disposal schedules.

As amended Pub.L. 91–287, § 4, June 23, 1970, 84 Stat. 322.

1970 Amendment. Pub.L. 91-287 struck out "approved by Congress" following "disposal schedules" in two instances.

Legislative History. For legislative history and purpose of Pub.L. 91-287, see 1970 U.S.Code Cong. and Adm.News, p. 3297.

CHAPTER 31—RECORDS MANAGEMENT BY FEDERAL AGENCIES

Code of Federal Regulations

Policies and procedures applicable for management of records, see 41 CFR 101-11.000 et seq.

CHAPTER 33.—DISPOSAL OF RECORDS

Sec.
3301. Definition of records.
3302. Regulations covering lists of records for disposal, procedure for disposal, and standards for reproduction; approval by President.
3303. Lists and schedules of records to be submitted to Administrator of General Services by head of each Government agency.
3303a. Examination by Administrator of General Services of lists and schedules of records lacking preservation value; disposal of records.
3308. Disposal of similar records where prior disposal was authorized.
3309. Preservation of claims of Government until settled in General Accounting Office; disposal authorized upon written approval of Comptroller General.
3310. Disposal of records constituting menace to health, life, or property.
3311. Destruction of records outside continental United States in time of war or when hostile action seems imminent; written report to Administrator of General Services.
3312. Photographs or microphotographs of records considered as originals; certified reproductions admissible in evidence.
3313. Moneys from sale of records payable into the Treasury.
3314. Procedures for disposal of records exclusive.

1970 Amendment. Pub.L. 91-287, § 3.

§ 3303a. Examination by Administrator of General Services of lists and schedules of records lacking preservation value; disposal of records

(a) The Administrator of General Services shall examine the lists and schedules submitted to him under section 3303 of this title. If the Administrator determines that any of the records listed in a list or schedule submitted to him do not, or will not after the lapse of the period specified, have sufficient administrative, legal, research, or other value to warrant their continued preservation by the Government, he may—

(1) notify the agency to that effect; and

(2) empower the agency to dispose of those records in accordance with regulations promulgated under section 3302 of this title.

(b) Authorizations granted under lists and schedules submitted to the Administrator under section 3303 of this title shall be mandatory, subject to section 2909 of this title. Authorizations granted under schedules promulgated under subsection (d) of this section shall be permissive.

(c) The Administrator may request advice and counsel from the Committee on Rules and Administration of the Senate and the Committee on House Administration of the House of Representatives with respect to the disposal of any particular records under this chapter whenever he considers that—

(1) those particular records may be of special interest to the Congress; or

(2) consultation with the Congress regarding the disposal of those particular records is in the public interest.

However, this subsection does not require the Administrator to request such advice and counsel as a regular procedure in the general disposal of records under this chapter.

(d) The Administrator may promulgate schedules authorizing the disposal, after the lapse of specified periods of time, of records of a specified form or character common to several or all agencies if such records will not, at the end of the periods specified, have sufficient administrative, legal, research, or other value to warrant their further preservation by the United States Government.

(e) The Administrator may approve and effect the disposal of records that are in his legal custody, provided that records that had been in the custody of another existing agency may not be disposed of without the written consent of the head of the agency.

(f) The Administrator shall make an annual report to the Congress concerning the disposal of records under this chapter, including general descriptions of the types of records disposed of and such other information as he considers appropriate to keep the Congress fully informed regarding the disposal of records under this chapter.

Added Pub.L. 91–287, § 1, June 23, 1970, 84 Stat. 320.

Legislative History. For legislative history and purpose of Pub.L. 91–287, see 1970 U.S.Code Cong. and Adm.News, p. 3287.

§§ 3304 to 3307. Repealed. Pub.L. 91–287, § 2(c) (1)–(4), June 23, 1970, 84 Stat. 321, 322

Sections, Pub.L. 90–620, Oct. 22, 1968, 82 Stat. 1300, 1301, related to disposal of records as follows:

Section 3304, submission to Congress by Administrator of General Services of lists and schedules of records lacking preservation value.

Section 3305, examination of lists and schedules by joint congressional committees and report to Congress.

Section 3306, disposal of records by head of Government agency upon notification by Administrator of action by joint congressional committee.

Section 3307, disposal of records upon failure of joint congressional committee to act.

Subject matter is now covered by section 3303a of this title, last sentence of first par. and second par. of former section 3304 of this title being covered by subsecs. (e) and (d) of section 3303a of this title, respectively.

§ 3308. Disposal of similar records where prior disposal was authorized

When it appears to the Administrator of General Services that an agency has in its custody, or is accumulating, records of the same form or character as those of the same agency previously authorized to be disposed of, he may empower the head of the agency to dispose of the records, after they have been in existence a specified period of time, in accordance with regulations promulgated under section 3302 of this title and without listing or scheduling them.

As amended Pub.L. 91–287, § 2(a), June 23, 1970, 84 Stat. 321.

1970 Amendment. Pub.L. 91-287 struck out "by Congress" following "authorized".

Legislative History. For legislative history and purpose of Pub.L. 91-287, see 1970 U.S.Code Cong. and Adm.News, p. 3297.

§ 3309. Preservation of claims of Government until settled in General Accounting Office; disposal authorized upon written approval of Comptroller General

Records pertaining to claims and demands by or against the Government of the United States or to accounts in which the Government of the United States is concerned, either as debtor or creditor, may not be disposed of by the head of an agency under authorization granted under this chapter, until the claims, demands, and accounts have been settled and adjusted in the General Accounting Office, except upon the written approval of the Comptroller General of the United States.

As amended Pub.L. 91–287, § 2(b), June 23, 1970, 84 Stat. 321.

1970 Amendment. Pub.L. 91-287 substituted "under this chapter" for "under sections 3306-3308 of this title".

Legislative History. For legislative history and purpose of Pub.L. 91-287, see 1970 U.S.Code Cong. and Adm.News, p. 3297.

CHAPTER 35.—COORDINATION OF FEDERAL REPORTING SERVICES

Sec.
[3512. Information for independent regulatory agencies] [1]

[1] Item 3512 has been editorially inserted. Section 3512 was enacted by Pub.L. 93-153 without a concurrent insertion into the chapter analysis.

§ 3502. Definitions

As used in this chapter—

"Federal agency" means an executive department, commission, independent establishment, corporation owned or controlled by the United States, board, bureau, division, service, office, authority, or administration in the executive branch of the Government; but does not include the General Accounting Office, independent Federal regulatory agencies, nor the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions;

"person" means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of persons, a State or territorial government or branch, or a political subdivision of a State or territory or a branch of a political subdivision;

"information" means facts obtained or solicited by the use of written report forms, application forms, schedules, questionnaires, or other similar methods calling either for answers to identical questions from ten or more persons other than agencies, instrumentalities, or employees of the United States or for answers to questions from agencies, instrumentalities, or employees of the United States which

are to be used for statistical compilations of general public interest.

As amended Pub.L. 93–153, Title IV, § 409(a), Nov. 16, 1973, 87 Stat. 593.

1973 Amendment. Pub.L. 93–153 inserted "independent Federal regulatory agencies," following "General Accounting Office" in the definition of "Federal agency".

Legislative History. For legislative history and purpose of Pub.L. 93–153, see 1973 U.S.Code Cong. and Adm.News, p. —.

§§ 3503, 3504, 3506, 3507, 3509, 3510

Office of Management and Budget. The Bureau of the Budget was designated as the Office of Management and Budget and offices of Director of the Bureau of the Budget, Deputy Director of the Bureau of the Budget, and Assistant Directors of the Bureau of the Budget were designated Director of the Office of Management and Budget, Deputy Director of the Office of Management and Budget, and Assistant Directors of the Office of Management and Budget, respectively. Records, property, personnel, and funds of the Bureau of the Budget were transferred to the Office of Management and Budget. See Part I of Reorganization Plan 2 of 1970, set out in the Appendix to Title 5, Government Organization and Employees.

§ 3512. Information for independent regulatory agencies

(a) The Comptroller General of the United States shall review the collection of information required by independent Federal regulatory agencies described in section 3502 of this chapter to assure that information required by such agencies is obtained with a minimum burden upon business enterprises, especially small business enterprises, and other persons required to furnish the information. Unnecessary duplication of efforts in obtaining information already filed with other Federal agencies or departments through the use of reports, questionnaires, and other methods shall be eliminated as rapidly as practicable. Information collected and tabulated by an independent regulatory agency shall, as far as is expedient, be tabulated in a manner to maximize the usefulness of the information to other Federal agencies and the public.

(b) In carrying out the policy of this section, the Comptroller General shall review all existing information gathering practices of independent regulatory agencies as well as requests for additional information with a view toward—

(1) avoiding duplication of effort by independent regulatory agencies, and

(2) minimizing the compliance burden on business enterprises and other persons.

(c) In complying with this section, an independent regulatory agency shall not conduct or sponsor the collection of information upon an identical item from ten or more persons, other than Federal employees, unless, in advance of adoption or revision of any plans or forms to be used in the collection—

(1) the agency submitted to the Comptroller General the plans or forms, together with the copies of pertinent regulations and of other related materials as the Comptroller General has specified; and

(2) the Comptroller General has advised that the information is not presently available to the independent agency from another source within the Federal Government and has determined that the proposed plans or forms are consistent with the provision of this section. The Comptroller General shall maintain facilities for carrying out the purposes of this section and shall render such advice to the requestive independent regulatory agency within forty-five days.

(d) While the Comptroller General shall determine the availability from other Federal sources of the information sought and the appropriateness of the forms for the collection of such information, the independent regulatory agency shall make the final determination as to the necessity of the information in carrying out its statutory respon-

sibilities and whether to collect such information. If no advice is received from the Comptroller General within forty-five days, the independent regulatory agency may immediately proceed to obtain such information.

(e) Section 3508(a) of this chapter dealing with unlawful disclosure of information shall apply to the use of information by independent regulatory agencies.

(f) The Comptroller General may promulgate rules and regulations necessary to carry out this chapter.

Added Pub.L. 93–153, Title IV, § 409(b), Nov. 16, 1973, 87 Stat. 593.

Legislative History. For legislative history and purpose of Pub.L. 93–153, see 1973 U.S.Code Cong. and Adm.News, p. —.

INDEX

CONSULT GENERAL INDEX POCKET PART

[345 U.S. 41 (1953)]

Syllabus.

UNITED STATES v. RUMELY.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT.

No. 87. Argued December 11–12, 1952.—Decided March 9, 1953.

Respondent was secretary of an organization which, among other things, engaged in the sale of books of a political nature. He refused to disclose to a committee of Congress the names of those who made bulk purchases of these books for further distribution, and was convicted under R. S. § 102, as amended, which provides penalties for refusal to give testimony or to produce relevant papers "upon any matter" under congressional inquiry. Under the resolution empowering it to function, the Committee was "authorized and directed to conduct a study and investigation of (1) all lobbying activities intended to influence, encourage, promote, or retard legislation; and (2) all activities of agencies of the Federal Government intended to influence, encourage, promote, or retard legislation." *Held:* The Committee was without power to exact the information sought from respondent. Pp. 42–48.

(a) To construe the resolution as authorizing the Committee to inquire into all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiations of influence which they may exert upon the ultimate legislative process, would raise doubts of constitutionality in view of the prohibition of the First Amendment. P. 46.

(b) The phrase "lobbying activities" in the resolution is to be construed as lobbying in the commonly accepted sense of "representations made directly to the Congress, its members, or its committees"; and not as extending to attempts "to saturate the thinking of the community." P. 47.

(c) The scope of the resolution defining respondent's duty to answer must be ascertained as of the time of his refusal and cannot be enlarged by subsequent action of Congress. Pp. 47–48.

90 U. S. App. D. C. 382, 197 F. 2d 166, affirmed.

Respondent was convicted under R. S. § 102, as amended, 2 U. S. C. § 192, for refusal to give certain information to a congressional committee. The Court of

Appeals reversed. 90 U. S. App. D. C. 382, 197 F. 2d 166. This Court granted certiorari. 344 U. S. 812. *Affirmed*, p. 48.

Oscar H. Davis argued the cause for the United States. With him on the main brief was *Robert L. Stern*, then Acting Solicitor General. With him on a reply brief was *Solicitor General Cummings. Assistant Attorney General Murray, Beatrice Rosenberg* and *John R. Wilkins* were on both briefs.

Donald R. Richberg argued the cause for respondent. With him on the brief were *Alfons B. Landa* and *Delmar W. Holloman.*

MR. JUSTICE FRANKFURTER delivered the opinion of the Court.

The respondent Rumely was Secretary of an organization known as the Committee for Constitutional Government, which, among other things, engaged in the sale of books of a particular political tendentiousness. He refused to disclose to the House Select Committee on Lobbying Activities the names of those who made bulk purchases of these books for further distribution, and was convicted under R. S. § 102, as amended, 52 Stat. 942, 2 U. S. C. § 192, which provides penalties for refusal to give testimony or to produce relevant papers "upon any matter" under congressional inquiry. The Court of Appeals reversed, one judge dissenting. It held that the committee before which Rumely refused to furnish this information had no authority to compel its production. 90 U. S. App. D. C. 382, 197 F. 2d 166. Since the Court of Appeals thus took a view of the committee's authority contrary to that adopted by the House in citing Rumely for contempt, we granted certiorari. 344 U. S. 812. This issue—whether the committee was authorized to

exact the information which the witness withheld—must first be settled before we may consider whether Congress had the power to confer upon the committee the authority which it claimed.

Although we are here dealing with a resolution of the House of Representatives, the problem is much the same as that which confronts the Court when called upon to construe a statute that carries the seeds of constitutional controversy. The potential constitutional questions have far-reaching import. We are asked to recognize the penetrating and pervasive scope of the investigative power of Congress. The reach that may be claimed for that power is indicated by Woodrow Wilson's characterization of it:

> "It is the proper duty of a representative body to look diligently into every affair of government and to talk much about what it sees. It is meant to be the eyes and the voice, and to embody the wisdom and will of its constituents. Unless Congress have and use every means of acquainting itself with the acts and the disposition of the administrative agents of the government, the country must be helpless to learn how it is being served; and unless Congress both scrutinize these things and sift them by every form of discussion, the country must remain in embarrassing, crippling ignorance of the very affairs which it is most important that it should understand and direct. The informing function of Congress should be preferred even to its legislative function." Wilson, Congressional Government, 303.

Although the indispensable "informing function of Congress" is not to be minimized, determination of the "rights" which this function implies illustrates the common juristic situation thus defined for the Court by Mr. Justice Holmes: "All rights tend to declare themselves

absolute to their logical extreme. Yet all in fact are limited by the neighborhood of principles of policy which are other than those on which the particular right is founded, and which become strong enough to hold their own when a certain point is reached." *Hudson Water Co.* v. *McCarter*, 209 U. S. 349, 355. President Wilson did not write in light of the history of events since he wrote; more particularly he did not write of the investigative power of Congress in the context of the First Amendment. And so, we would have to be that "blind" Court, against which Mr. Chief Justice Taft admonished in a famous passage, *Child Labor Tax Case*, 259 U. S. 20, 37, that does not see what "[a]ll others can see and understand" not to know that there is wide concern, both in and out of Congress, over some aspects of the exercise of the congressional power of investigation.

Accommodation of these contending principles—the one underlying the power of Congress to investigate, the other at the basis of the limitation imposed by the First Amendment—is not called for until after we have construed the scope of the authority which the House of Representatives gave to the Select Committee on Lobbying Activities. The pertinent portion of the resolution of August 12, 1949, reads:

> "The committee is authorized and directed to conduct a study and investigation of (1) all lobbying activities intended to influence, encourage, promote, or retard legislation; and (2) all activities of agencies of the Federal Government intended to influence, encourage, promote, or retard legislation." H. Res. 298, 81st Cong., 1st Sess.

This is the controlling charter of the committee's powers. Its right to exact testimony and to call for the production of documents must be found in this language. The resolution must speak for itself, since Congress put

no gloss upon it at the time of its passage. Nor is any help to be had from the fact that the purpose of the Buchanan Committee, as the Select Committee was known, was to try to "find out how well [the Federal Regulation of Lobbying Act of 1946, 60 Stat. 839] worked." 96 Cong. Rec. 13882. That statute had a section of definitions, but Congress did not define the terms "lobbying" or "lobbying activities" in that Act, for it did not use them. Accordingly, the phrase "lobbying activities" in the resolution must be given the meaning that may fairly be attributed to it, having special regard for the principle of constitutional adjudication which makes it decisive in the choice of fair alternatives that one construction may raise serious constitutional questions avoided by another. In a long series of decisions we have acted on this principle. In the words of Mr. Chief Justice Taft, "[i]t is our duty in the interpretation of federal statutes to reach a conclusion which will avoid serious doubt of their constitutionality." *Richmond Co.* v. *United States*, 275 U. S. 331, 346. Again, what Congress has written, we said through Mr. Chief Justice (then Mr. Justice) Stone, "must be construed with an eye to possible constitutional limitations so as to avoid doubts as to its validity." *Lucas* v. *Alexander*, 279 U. S. 573, 577. As phrased by Mr. Chief Justice Hughes, "if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided." *Crowell* v. *Benson*, 285 U. S. 22, 62, and cases cited.

Patently, the Court's duty to avoid a constitutional issue, if possible, applies not merely to legislation technically speaking but also to congressional action by way of resolution. See *Federal Trade Comm'n* v. *American Tobacco Co.*, 264 U. S. 298. Indeed, this duty of not

needlessly projecting delicate issues for judicial pronouncement is even more applicable to resolutions than to formal legislation. It can hardly be gainsaid that resolutions secure passage more casually and less responsibly, in the main, than do enactments requiring presidential approval.

Surely it cannot be denied that giving the scope to the resolution for which the Government contends, that is, deriving from it the power to inquire into all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiations of influence which they may exert upon the ultimate legislative process, raises doubts of constitutionality in view of the prohibition of the First Amendment. In light of the opinion of Prettyman, J., below and of some of the views expressed here, it would not be seemly to maintain that these doubts are fanciful or factitious. Indeed, adjudication here, if it were necessary, would affect not an evanescent policy of Congress, but its power to inform itself, which underlies its policy-making function. Whenever constitutional limits upon the investigative power of Congress have to be drawn by this Court, it ought only to be done after Congress has demonstrated its full awareness of what is at stake by unequivocally authorizing an inquiry of dubious limits. Experience admonishes us to tread warily in this domain. The loose language of *Kilbourn* v. *Thompson*, 103 U. S. 168, the weighty criticism to which it has been subjected, see, *e. g.*, Fairman, Mr. Justice Miller and the Supreme Court, 332–334; Landis, Constitutional Limitations on the Congressional Power of Investigation, 40 Harv. L. Rev. 153, the inroads that have been made upon that case by later cases, *McGrain* v. *Daugherty*, 273 U. S. 135, 170–171, and *Sinclair* v. *United States*, 279 U. S. 263, strongly counsel abstention from adjudication unless no choice is left.

Choice is left. As a matter of English, the phrase "lobbying activities" readily lends itself to the construction placed upon it below, namely, "lobbying in its commonly accepted sense," that is, "representations made directly to the Congress, its members, or its committees," 90 U. S. App. D. C. 382, 391, 197 F. 2d 166, 175, and does not reach what was in Chairman Buchanan's mind, attempts "to saturate the thinking of the community." 96 Cong. Rec. 13883. If "lobbying" was to cover all activities of anyone intending to influence, encourage, promote or retard legislation, why did Congress differentiate between "lobbying activities" and other "activities . . . intended to influence"? Had Congress wished to authorize so extensive an investigation of the influences that form public opinion, would it not have used language at least as explicit as it employed in the very resolution in question in authorizing investigation of government agencies? Certainly it does no violence to the phrase "lobbying activities" to give it a more restricted scope. To give such meaning is not barred by intellectual honesty. So to interpret is in the candid service of avoiding a serious constitutional doubt. "Words have been strained more than they need to be strained here in order to avoid that doubt." (Mr. Justice Holmes in *Blodgett* v. *Holden*, 275 U. S. 142, 148, with the concurrence of Mr. Justice Brandeis, Mr. Justice Sanford and Mr. Justice Stone.) With a view to observing this principle of wisdom and duty, the Court very recently strained words more than they need be strained here. *United States* v. *C. I. O.*, 335 U. S. 106. The considerations which prevailed in that case should prevail in this.

Only a word need be said about the debate in Congress after the committee reported that Rumely had refused to produce the information which he had a right to refuse under the restricted meaning of the phrase "lobbying activities." The view taken at that time by the committee and by the Congress that the committee was au-

thorized to ask Rumely for the information he withheld is not legislative history defining the scope of a congressional measure. What was said in the debate on August 30, 1950, after the controversy had arisen regarding the scope of the resolution of August 12, 1949, had the usual infirmity of *post litem motam*, self-serving declarations.[1] In any event, Rumely's duty to answer must be judged as of the time of his refusal. The scope of the resolution defining that duty is therefore to be ascertained as of that time and cannot be enlarged by subsequent action of Congress.

Grave constitutional questions are matters properly to be decided by this Court but only when they inescapably come before us for adjudication. Until then it is our duty to abstain from marking the boundaries of congressional power or delimiting the protection guaranteed by the First Amendment. Only by such self-restraint will we avoid the mischief which has followed occasional departures from the principles which we profess.

The judgment below should be

Affirmed.

MR. JUSTICE BURTON and MR. JUSTICE MINTON took no part in the consideration or decision of this case.

MR. JUSTICE DOUGLAS, with whom MR. JUSTICE BLACK concurs, concurring.

Respondent was convicted under an indictment charging willful refusal to produce records and give testimony before a Committee of the House of Representatives in violation of R. S. § 102, as amended, 52 Stat. 942, 2

[1] The ambiguity of the terms of the resolution—that is, whether questions asked to which answers were refused were within those terms—is reflected by the close division by which the committee's view of its own authority prevailed. The vote was 183 to 175.

U. S. C. § 192.[1] The Committee, known as the Select Committee on Lobbying Activities, was created on August 12, 1949, by House Resolution 298[2] which provides in part as follows:

> "The committee is authorized and directed to conduct a study and investigation of (1) all lobbying activities intended to influence, encourage, promote, or retard legislation; and (2) all activities of agencies of the Federal Government intended to influence, encourage, promote, or retard legislation."

Count one of the indictment charged that respondent willfully refused to produce records, duly subpoenaed, of the Committee for Constitutional Government (CCG), showing the name and address of each person from whom a total of $1,000 or more had been received by CCG from January 1, 1947, to May 1, 1950, for any purpose *including receipts from the sale of books and pamphlets.* Count six charged a similar offense as to a subpoena calling for the name and address of each person from whom CCG had received between those dates a total of $500 or more *for any purpose.* Count seven charged a willful refusal to give the name of a woman from Toledo who gave respondent $2,000 for distribution of The Road Ahead, a book written by John T. Flynn.

The background of the subpoena and of the questions asked respondent is contained in a report of the Select

---

[1] This section provides in pertinent part: "Every person who having been summoned as a witness by the authority of either House of Congress to give testimony or to produce papers upon any matter under inquiry before either House, . . . or any committee of either House of Congress, willfully makes default, or who, having appeared, refuses to answer any question pertinent to the question under inquiry, shall be deemed guilty of a misdemeanor, punishable by a fine of not more than $1,000 nor less than $100 and imprisonment in a common jail for not less than one month nor more than twelve months."

[2] H. Res. 298, 81st Cong., 1st Sess.

Committee, H. R. Rep. No. 3024, 81st Cong., 2d Sess. It appears that CCG and respondent, its executive, registered under the Regulation of Lobbying Act (60 Stat. 839, 2 U. S. C. §§ 261 *et seq.*) on October 7, 1946. The reports under this registration (which was made under protest) showed that CCG had spent about $2,000,000 from October 1946 to August 1950. The basic function of CCG, according to the Select Committee, was the "distribution of printed material to influence legislation indirectly." The Regulation of Lobbying Act requires disclosure of contributions of $500 or more received or expended to influence, directly or indirectly, the passage or defeat of any legislation by the Congress. 2 U. S. C. §§ 264, 266. The Select Committee reported that after enactment of the Regulation of Lobbying Act CCG adopted a policy of accepting payments of over $490 only if the contributor specified that the funds be used for the distribution of one or more of its books or pamphlets. It then applied the term "sale" to the "contribution" and did not report them under the Regulation of Lobbying Act. H. R. Rep. No. 3024, *supra,* pp. 1, 2.

The Report of the Select Committee also shows that while respondent was willing to give the Committee the total income of CCG, he refused to reveal the identity of the purchasers of books and literature because "under the Bill of Rights, that is beyond the power of your committee to investigate." *Id.*, p. 8. The books involved were The Road Ahead by John T. Flynn, The Constitution of the United States by Thomas J. Norton, Compulsory Medical Care and the Welfare State, by Melchior Palyi, and Why the Taft-Hartley Law by Irving B. McCann. Most of the purchasers (about 90 percent) had the books shipped to themselves; the rest told CCG the individuals to send them to or the type of person (*e. g.*, "farm leaders") who should receive them. One person had CCG send Com-

pulsory Medical Care by Melchior Palyi to 15,550 libraries.[3]

The Select Committee stated in its report:

> "Our study of this organization indicates very clearly that its most important function is the distribution of books and pamphlets in order to influence legislation directly and indirectly. It attempts to influence legislation directly by sending copies of books, pamphlets, and other printed materials to Members of Congress. It attempts to influence legislation indirectly by distributing hundreds of thousands of copies of these printed materials to people throughout the United States.
>
> "Of particular significance is the fact that Edward A. Rumely and the Committee for Constitutional Government, Inc., in recent years have devised a scheme for raising enormous funds without filing true reports pursuant to the provisions of the Federal Regulation of Lobbying Act. This scheme has the color of legality but in fact is a method of circumventing the law. It utilizes the system outlined above whereby contributions to the Committee for Constitutional Government are designated as payments for the purchase of books, which are transmitted to others at the direction of the purchaser, with both the contributor of the money and the recipients of the books totally unaware of the subterfuge in most cases." H. R. Rep. No. 3024, *supra*, p. 2.

---

[3] When the Taft-Hartley law was under discussion, CCG published a pamphlet "Labor Monopolies or Freedom" of which 250,000 copies were distributed. "All members of Congress got a copy. It went to publishers. People who could take opinion that way, and mint it into small coin to distribute to others." H. R. Rep. No. 3024, *supra*, p. 11. Respondent testified that Frank Gannett paid for that distribution.

The Select Committee insisted that the information demanded of respondent was relevant to its investigation of "lobbying activities" within the meaning of the Resolution. It said:

> "Because of the refusal of the Committee for Constitutional Government, Inc., to produce pertinent financial records, this committee was unable to determine whether or not the Committee for Constitutional Government, Inc., is evading or violating the letter or the spirit of the Federal Regulation of Lobbying Act by the establishment of [a] class [of] contributions called 'Receipts from the sale of books and literature,' or whether they are complying with a law which requires amendments to strengthen it.
>
> "The policy of the Committee for Constitutional Government, Inc., of refusing to accept contributions of more than $490 unless earmarked for books, etc., may also involve: (1) Dividing large contributions into installments of $490 or less, and causing the records of the Committee for Constitutional Government to reflect receipt of each installment on a different date, and/or causing the records of the Committee for Constitutional Government to give credit, for the several installments, to various relatives and associates of the actual contributor. (2) Causing the Committee for Constitutional Government's records as to 'Contributions' to reflect less than the total amount of contributions actually received, by labeling some part of such funds as payments made for printed matter.
>
> "Because of the refusal of the Committee for Constitutional Government, Inc., to produce pertinent financial records, this committee was unable to determine whether or not the Federal Regulation of Lobbying Act requires amendment to prevent division of

large contributions into installments, or to prevent the crediting of contributions to others than the real contributor, or to prevent the use of other subterfuges." H. R. Rep. No. 3024, *supra*, pp. 2–3.

The Select Committee submitted its report to the House (96 Cong. Rec. 13873) and offered a Resolution that the Speaker certify respondent's refusal to answer to the United States Attorney for the District of Columbia. *Id.*, p. 13881. The House adopted the Resolution, *id.*, p. 13893, and on August 31, 1950, the Speaker certified respondent's refusal to testify.

Respondent was convicted and sentenced to a fine of $1,000 and to imprisonment for six months. The Court of Appeals reversed by a divided vote (90 U. S. App. D. C. 382, 197 F. 2d 166), the majority holding that "lobbying activities" as used in the Resolution creating the Select Committee did not authorize the inquiries made of respondent. In its view the term "lobbying activities" meant direct contact with Congress, not attempts to influence public opinion through the sale of books and documents.

I.

The Court holds that Resolution 298 which authorized the Select Committee to investigate "lobbying activities" did not extend to the inquiry on which this contempt proceeding is based. The difficulty with that position starts with Resolution 298. Its history makes plain that it was intended to probe the sources of support of lobbyists registered under the Regulation of Lobbying Act. Congressman Sabath, one of the sponsors of the Resolution, included CCG in a "partial list of some of the large lobby organizations and their reports of expenditures for the first quarter of 1949." See 95 Cong. Rec., p. 11386. The Regulation of Lobbying Act, under which respondent and CCG were registered, applies to all persons soliciting

or receiving money to be used principally "to influence, directly or indirectly, the passage or defeat of any legislation by the Congress of the United States." 2 U. S. C. § 266 (b). Congressman Buchanan, who introduced the Resolution and who became Chairman of the Select Committee, said that the purpose of the Resolution was to investigate the operations of that Act.[4] Not a word in the Resolution, not a word in the debate preceding its adoption suggests that the inquiry was to be delimited, restricted, or confined to particular methods of collecting money to influence legislation directly or indirectly.

The Select Committee took the same broad view of its authority.[5] It concluded that "all substantial attempts to influence legislation for pay or for any consideration constitute lobbying." H. R. Rep. No. 3239, 81st Cong., 2d Sess., p. 1. It said that "pamphleteering" was a lobbying activity that overshadows "the traditional techniques of contact and persuasion." *Id.*, p. 3. And it cited for its conclusion the activities of CCG. *Id.* This conclusion was reached over vehement objections by three minority members of the Select Committee who insisted that an investigation of that breadth exceeded the authority of the Resolution and infringed on the constitutional rights of free speech and free press. *Id.*, Part 2, p. 2.

---

[4] "Pressure groups interpret the Lobbying Act in different ways. Some file expenses. Others file full budget, but list expenditures they judge allocable to legislative activities. Still others file only expenditures directly concerned with lobbying.

"Some organizations argue they need not file unless principal purpose is influencing legislation. But Justice Department says, 'principal' includes all who have substantial legislative interests. Lobbies also differ on who filed expenditures—organizations or individuals." 95 Cong. Rec. 11389.

[5] An analysis of the scope of the investigation and the meaning of "lobbying" is contained in the General Interim Report of the Select Committee. H. R. Rep. No. 3138, 81st Cong., 2d Sess., pp. 5 *et seq.*

This was the posture of the case when the Select Committee referred respondent's refusal to testify to the House for contempt proceedings. Congressman Buchanan called the collection of funds through the sale of books and pamphlets an evasion of the Regulation of Lobbying Act. 96 Cong. Rec. 13882. He pressed on the House the importance of controlling that kind of activity in a regulation of lobbying. And he asked that the House ratify the conclusion of the Select Committee that respondent was in contempt. *Id.*, pp. 13886, 13887. That construction of the Resolution was challenged by Congressman Halleck, a member of the Select Committee who signed the minority report. He argued that the contempt citation sought had "nothing to do with the influencing of legislation in the ordinary ways of seeing Members of Congress or communicating with them. It has only to do with the formation of public opinion among the people of the country." *Id.*, p. 13888. Congressman Halleck's argument was twofold—that the inquiry was not within the purview of the Resolution and that, if it were, it would be unconstitutional. *Id.*, pp. 13887–13888. Others took up the debate on those issues. The vote was taken; and the Resolution passed. *Id.*, p. 13893.

Thus the House had squarely before it the meaning of its earlier Resolution. A narrower construction than the Select Committee adopted was urged upon it. Congressmen pleaded long and earnestly for the narrow construction and pointed out that, if the broader interpretation were taken, the inquiry would be trenching on the constitutional rights of citizens. I cannot say, in the face of that close consideration of the question by the House itself, that the Select Committee exceeded its authority. The House of Representatives made known its construction of the powers it had granted. If at the beginning there were any doubts as to the meaning of

Resolution 298, the House removed them. The Court is repudiating what the House emphatically affirmed, when it now says that the Select Committee lacked the authority to compel respondent to answer the questions propounded.

II.

Of necessity I come then to the constitutional questions. Respondent represents a segment of the American press. Some may like what his group publishes; others may disapprove. These tracts may be the essence of wisdom to some; to others their point of view and philosophy may be anathema. To some ears their words may be harsh and repulsive; to others they may carry the hope of the future. We have here a publisher who through books and pamphlets seeks to reach the minds and hearts of the American people. He is different in some respects from other publishers. But the differences are minor. Like the publishers of newspapers, magazines, or books, this publisher bids for the minds of men in the market place of ideas. The aim of the historic struggle for a free press was "to establish and preserve the right of the English people to full information in respect of the doings or misdoings of their government." *Grosjean* v. *American Press Co.*, 297 U. S. 233, 247. That is the tradition behind the First Amendment. Censorship or previous restraint is banned. *Near* v. *Minnesota*, 283 U. S. 697. Discriminatory taxation is outlawed. *Grosjean* v. *American Press Co.*, *supra*. The privilege of pamphleteering, as well as the more orthodox types of publications, may neither be licensed (*Lovell* v. *Griffin*, 303 U. S. 444) nor taxed. *Murdock* v. *Pennsylvania*, 319 U. S. 105. Door to door distribution is privileged. *Martin* v. *Struthers*, 319 U. S. 141. These are illustrative of the preferred position granted speech and the press by the First Amendment. The command that "Congress

shall make no law . . . abridging the freedom of speech, or of the press" has behind it a long history. It expresses the confidence that the safety of society depends on the tolerance of government for hostile as well as friendly criticism, that in a community where men's minds are free, there must be room for the unorthodox as well as the orthodox views.

If the present inquiry were sanctioned, the press would be subjected to harassment that in practical effect might be as serious as censorship. A publisher, compelled to register with the Federal Government, would be subjected to vexatious inquiries. A requirement that a publisher disclose the identity of those who buy his books, pamphlets, or papers is indeed the beginning of surveillance of the press. True, no legal sanction is involved here. Congress has imposed no tax, established no board of censors, instituted no licensing system. But the potential restraint is equally severe. The finger of government leveled against the press is ominous. Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads. The purchase of a book or pamphlet today may result in a subpoena tomorrow. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike. When the light of publicity may reach any student, any teacher, inquiry will be discouraged. The books and pamphlets that are critical of the administration, that preach an unpopular policy in domestic or foreign affairs, that are in disrepute in the orthodox school of thought will be suspect and subject to investigation. The press and its readers will pay a heavy price in harassment. But that will be minor in comparison with the menace of

37-583 O - 74 - pt. 2 - 17

[400 U. S. 433 (1971)]

Syllabus

WISCONSIN *v.* CONSTANTINEAU

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF WISCONSIN

No. 95. Argued December 10, 1970—Decided January 19, 1971

The police chief of Hartford, Wisconsin, pursuant to a state statute, caused to be posted a notice in all retail liquor outlets in Hartford that sales or gifts of liquor to appellee, a resident of that city, were forbidden for one year. The statute provides for such "posting," without notice or hearing, with respect to any person who "by excessive drinking" produces certain conditions or exhibits specified traits, such as exposing himself or family "to want" or becoming "dangerous to the peace" of the community. On appellee's suit seeking, *inter alia*, injunctive relief, a three-judge federal court held the statute unconstitutional as violative of procedural due process. *Held:*

1. The label or characterization given an individual by "posting," though a mark of serious illness to some, is to others such a stigma or badge of disgrace that procedural due process requires notice and an opportunity to be heard. Pp. 436–437.

2. Since here the state statute is unambiguous and there is no uncertain issue of state law, the federal court properly proceeded to determine the federal constitutional claim. *Zwickler* v. *Koota*, 389 U. S. 241, 250–251. Pp. 437–439.

302 F. Supp. 861, affirmed.

DOUGLAS, J., delivered the opinion of the Court, in which HARLAN, BRENNAN, STEWART, WHITE, and MARSHALL, JJ., joined. BURGER, C. J., filed a dissenting opinion, in which BLACKMUN, J., joined, *post*, p. 439. BLACK, J., filed a dissenting opinion, in which BLACKMUN, J., joined, *post*, p. 443.

Benjamin Southwick, Assistant Attorney General of Wisconsin, argued the cause for appellant. With him on the brief were *Robert W. Warren*, Attorney General, and *Robert D. Martinson*, Assistant Attorney General.

S. A. Schapiro argued the cause and filed a brief for appellee.

the shadow which government will cast over literature that does not follow the dominant party line. If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, book stores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press. Congress could not do this by law. The power of investigation is also limited.[6] Inquiry into personal and private affairs is precluded. See *Kilbourn* v. *Thompson*, 103 U. S. 168, 190; *McGrain* v. *Daugherty*, 273 U. S. 135, 173–174; *Sinclair* v. *United States*, 279 U. S. 263, 292. And so is any matter in respect to which no valid legislation could be had. *Kilbourn* v. *Thompson, supra*, pp. 194–195; *McGrain* v. *Daugherty, supra*, p. 171. Since Congress could not by law require of respondent what the House demanded, it may not take the first step in an inquiry ending in fine or imprisonment.

---

[6] Cf. *Barsky* v. *United States*, 83 U. S. App. D. C. 127, 167 F. 2d 241, certiorari denied, 334 U. S. 843, rehearing denied, 339 U. S. 971, and *Marshall* v. *United States*, 85 U. S. App. D. C. 184, 176 F. 2d 473, certiorari denied, 339 U. S. 933, rehearing denied, 339 U. S. 959.

Opinion of the Court

MR. JUSTICE DOUGLAS delivered the opinion of the Court.

Appellee is an adult resident of Hartford, Wis. She brought suit in a federal district court in Wisconsin to have a Wisconsin statute declared unconstitutional.[1] A three-judge court was convened, 28 U. S. C. § 2281. That court, by a divided vote, held the Act unconstitutional, 302 F. Supp. 861, and we noted probable jurisdiction. 397 U. S. 985.

The Act, Wis. Stat. § 176.26 (1967), provides that designated persons may in writing forbid the sale or gift of intoxicating liquors to one who "by excessive drinking" produces described conditions or exhibits specified traits, such as exposing himself or family "to want" or becoming "dangerous to the peace" of the community.[2]

---

[1] 28 U. S. C. § 1343 provides: "The district courts shall have original jurisdiction of any civil action authorized by law to be commenced by any person . . . . (3) To redress the deprivation, under color of any State law, statute, ordinance, regulation, custom or usage, of any right, privilege or immunity secured by the Constitution of the United States or by any Act of Congress providing for equal rights of citizens or of all persons within the jurisdiction of the United States."

[2] Section 176.26 reads as follows:

"(1) When any person shall by excessive drinking of intoxicating liquors, or fermented malt beverages misspend, waste or lessen his estate so as to expose himself or family to want, or the town, city, village or county to which he belongs to liability for the support of himself or family, or so as thereby to injure his health, endanger the loss thereof, or to endanger the personal safety and comfort of his family or any member thereof, or the safety of any other person, or the security of the property of any other person, or when any person shall, on account of the use of intoxicating liquors or fermented malt beverages, become dangerous to the peace of any community, the wife of such person, the supervisors of such town, the mayor, chief of police or aldermen of such city, the trustees of such village, the county superintendent of the poor of such county, the chairman of the county board of supervisors of such county, the

The chief of police of Hartford, without notice or hearing to appellee, caused to be posted a notice in all retail liquor outlets in Hartford that sales or gifts of liquors to appellee were forbidden for one year. Thereupon this suit was brought against the chief of police claiming damages and asking for injunctive relief. The State of Wisconsin intervened as a defendant on the injunctive phase of the case and that was the only issue tried and decided, the three-judge court holding the Act unconstitutional on its face and enjoining its enforcement. The court said:

> "In 'posting' an individual, the particular city official or spouse is doing more than denying him the ability to purchase alcoholic beverages within

---

district attorney of such county or any of them, may, in writing signed by her, him or them, forbid all persons knowingly to sell or give away to such person any intoxicating liquors or fermented malt beverages, for the space of one year and in like manner may forbid the selling, furnishing, or giving away of any such liquors or fermented malt beverages, knowingly to such person by any person in any town, city or village to which such person may resort for the same. A copy of said writing so signed shall be personally served upon the person so intended to be prohibited from obtaining any such liquor or beverage.

"(2) And the wife of such person, the supervisors of any town, the aldermen of any city, the trustees of any village, the county superintendent of the poor of such county, the mayor of any city, the chairman of the county board of supervisors of such county, the district attorney or sheriff of such county, may, by a notice made and signed as aforesaid, in like manner forbid all persons in such town, city or village, to sell or give away intoxicating liquors or drinks or fermented malt beverages to any person given to the excessive use of such liquors, drinks or beverages, specifying such person, and such notice shall have the same force and effect when such specified person is a nonresident as is herein provided when such specified person is a resident of said town, city or village."

Section 176.28 makes the sale or gift of liquor to such a person a misdemeanor.

> the city limits. In essence, he is giving notice to the public that he has found the particular individual's behavior to fall within one of the categories enumerated in the statutes. It would be naive not to recognize that such 'posting' or characterization of an individual will expose him to public embarrassment and ridicule, and it is our opinion that procedural due process requires that before one acting pursuant to State statute can make such a quasi-judicial determination, the individual involved must be given notice of the intent to post and an opportunity to present his side of the matter." 302 F. Supp., at 864.

We have no doubt as to the power of a State to deal with the evils described in the Act. The police power of the States over intoxicating liquors was extremely broad even prior to the Twenty-first Amendment. *Crane* v. *Campbell*, 245 U. S. 304. The only issue present here is whether the label or characterization given a person by "posting," though a mark of serious illness to some, is to others such a stigma or badge of disgrace that procedural due process requires notice and an opportunity to be heard. We agree with the District Court that the private interest is such that those requirements of procedural due process must be met.

It is significant that most of the provisions of the Bill of Rights are procedural, for it is procedure that marks much of the difference between rule by law and rule by fiat.

We reviewed in *Cafeteria Workers* v. *McElroy*, 367 U. S. 886, 895, the nature of the various "private interest[s]" that have fallen on one side or the other of the line. See also *Sniadach* v. *Family Finance Corp.*, 395 U. S. 337, 339–342. Generalizations are hazardous as some state and federal administrative procedures are sum-

mary by reason of necessity or history. Yet certainly where the State attaches "a badge of infamy" to the citizen, due process comes into play. *Wieman* v. *Updegraff*, 344 U. S. 183, 191. "[T]he right to be heard before being condemned to suffer grievous loss of any kind, even though it may not involve the stigma and hardships of a criminal conviction, is a principle basic to our society." *Anti-Fascist Committee* v. *McGrath*, 341 U. S. 123, 168 (Frankfurter, J., concurring).

Where a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential. "Posting" under the Wisconsin Act may to some be merely the mark of illness, to others it is a stigma, an official branding of a person. The label is a degrading one. Under the Wisconsin Act, a resident of Hartford is given no process at all. This appellee was not afforded a chance to defend herself. She may have been the victim of an official's caprice. Only when the whole proceedings leading to the pinning of an unsavory label on a person are aired can oppressive results be prevented.

It is suggested that the three-judge court should have stayed its hand while the aggrieved person repaired to the state courts to obtain a construction of the Act or relief from it. The fact that Wisconsin does not raise the point does not, of course, mean that it lacks merit. Yet the suggestion is not in keeping with the precedents.

Congress could of course have routed all federal constitutional questions through the state court systems, saving to this Court the final say when it came to review of the state court judgments. But our First Congress [3] resolved differently and created the federal court system and in time granted the federal courts various heads of

[3] The First Judiciary Act is in 1 Stat. 73.

jurisdiction,[4] which today involve most federal constitutional rights. Once that jurisdiction was granted, the federal courts resolved those questions even when they were enmeshed with state law questions. In 1941 we gave vigor to the so-called abstention doctrine in *Railroad Commission* v. *Pullman Co.*, 312 U. S. 496. In that case an authoritative resolution of a knotty state law question might end the litigation and not give rise to any federal constitutional claim. *Id.*, at 501. We, therefore, directed the District Court to retain the suit pending a determination by a state court of the underlying state law question. We applied the abstention doctrine most recently in *Fornaris* v. *Ridge Tool Co.*, *ante*, at 44, where a relatively new Puerto Rican statute, which had not been authoritatively construed by the Commonwealth's courts, "might be judicially confined to a more narrow ambit which would avoid all constitutional questions." We ordered the federal courts to stay their hands until the Puerto Rican courts had spoken. Speaking of *Reetz* v. *Bozanich*, 397 U. S. 82, we noted that the "three-judge federal court should not have proceeded to strike down an Alaska law which, if construed by the Alaska Supreme Court, might be so confined as not to have any constitutional infirmity." *Ante*, at 43. But the abstention rule only applies where "the issue of state law is uncertain." *Harman* v. *Forssenius*, 380 U. S. 528, 534. Thus our abstention cases have dealt with unresolved questions of state law which only a state tribunal could authoritatively construe. *Reetz* v. *Bozanich*, *supra*; *City*

---

[4] 28 U. S. C. § 1343 (3) involved in the present case came into the statutes in 1871. 17 Stat. 13. In 1875 Congress enlarged federal jurisdiction by authorizing the "federal question" jurisdiction presently contained in 28 U. S. C. § 1331. See 18 Stat. 470. We recently reviewed this history in *Zwickler* v. *Koota*, 389 U. S. 241, 245–248.

of Meridian v. *Southern Bell Tel. & Tel. Co.*, 358 U. S. 639.

In the present case the Wisconsin Act does not contain any provision whatsoever for notice and hearing. There is no ambiguity in the state statute. There are no provisions which could fairly be taken to mean that notice and hearing might be given under some circumstances or under some construction but not under others. The Act on its face gives the chief of police the power to do what he did to the appellee. Hence the naked question, uncomplicated by an unresolved state law, is whether that Act on its face is unconstitutional. As we said in *Zwickler* v. *Koota*, 389 U. S. 241, 251, abstention should not be ordered merely to await an attempt to vindicate the claim in a state court. Where there is no ambiguity in the state statute, the federal court should not abstain but should proceed to decide the federal constitutional claim. *Id.*, at 250–251. We would negate the history of the enlargement of the jurisdiction of the federal district courts,[5] if we held the federal court should stay its hand and not decide the question before the state courts decided it.

Affirmed.

MR. CHIEF JUSTICE BURGER, with whom MR. JUSTICE BLACKMUN joins, dissenting.

The Court today strikes down, as unconstitutional, a Wisconsin statute that has never been challenged or tested in the Wisconsin state courts. The judges of Wisconsin probably will be taken by surprise by our summary action since few, if any, have ever heard of this case.

---

[5] See n. 4, *supra*.

Very likely we reach a correct result since the Wisconsin statute appears, on its face and in its application, to be in conflict with accepted concepts of due process.

The reason for my dissent is that it seems to me a very odd business to strike down a state statute, on the books for almost 40 years, without any opportunity for the state courts to dispose of the problem either under the Wisconsin Constitution or the U. S. Constitution. For all we know, the state courts would find this statute invalid under the State Constitution,[1] but no one on either side of the case thought to discuss this or exhibit any interest in the subject. Since no one could reasonably think that the judges of Wisconsin have less fidelity to due process requirements of the Federal Constitution than we do, this case is, for me, a classic illustration of one in which we should decline to act until resort to state courts has been exhausted. At oral argument counsel for Mrs. Constantineau was candid in saying that he had deliberately avoided resort to the state courts because he could secure, and indeed did secure, a three-judge federal district court to decide the issue and, in that posture, appeal would lie directly to this Court.

Only recently in the 1969 Term we held unanimously that a challenge, under the Equal Protection Clause of the Fourteenth Amendment and under certain provisions of the Alaska Constitution, to the constitutionality of a state statute restricting commercial salmon fishing licenses should not have been decided by the federal district court until the courts of Alaska had acted. There,

[1] Although Wisconsin has no due process clause as such, Art. I, § 1, of the Wisconsin Constitution has been held by the Wisconsin Supreme Court to be substantially equivalent to the limitation on state action contained in the Due Process and Equal Protection Clauses of the Fourteenth Amendment. *Pauly* v. *Keebler*, 175 Wis. 428, 185 N. W. 554 (1921).

as here, the statute's challenger wanted to use the "short cut" Congress has authorized. As here, the "short cut" was to convene a three-judge federal district court which held the Alaska statute invalid. Notwithstanding that the license applicants presented a sound claim, MR. JUSTICE DOUGLAS, speaking for a unanimous Court, said:

> "We are advised that the provisions of the Alaska Constitution at issue have never been interpreted by an Alaska court. The District Court, feeling sure of its grounds on the merits, held, however, that this was not a proper case for abstention, saying that 'if the question had been presented to an Alaska court, it would have shared our conviction that the challenged gear licensing scheme is not supportable.' 297 F. Supp., at 304. The three-judge panel was a distinguished one, two being former Alaska lawyers. And they felt that prompt decision was necessary to avoid the 'grave and irreparable' injury to the 'economic livelihood' of the appellees which would result, if they could not engage in their occupation 'during this year's forthcoming fishing season.' *Ibid.*
>
> "It is, of course, true that abstention is not necessary whenever a federal court is faced with a question of local law, the classic case being *Meredith* v. *Winter Haven*, 320 U. S. 228, where federal jurisdiction was based on diversity only. Abstention certainly involves duplication of effort and expense and an attendant delay. See *England* v. *Louisiana State Board*, 375 U. S. 411. That is why we have said that this judicially created rule which stems from *Railroad Comm'n* v. *Pullman Co.*, 312 U. S. 496, should be applied only where 'the issue of state law is uncertain.' *Harman* v. *Forssenius*, 380 U. S. 528, 534." *Reetz* v. *Bozanich*, 397 U. S. 82, 86 (1970).

This very wise doctrine is an essential one of policy and is a keystone of federalism. Previously this Court had underscored this concept, saying:

> "Proper exercise of federal jurisdiction requires that controversies involving unsettled questions of state law be decided in the state tribunals preliminary to a federal court's consideration of the underlying federal constitutional questions. . . . In such a case, when the state court's interpretation of the statute or evaluation of its validity under the state constitution may obviate any need to consider its validity under the Federal Constitution, the federal court should hold its hand, lest it render a constitutional decision unnecessarily." *City of Meridian* v. *Southern Bell Tel. & Tel. Co.*, 358 U. S. 639, 640–641 (1959).

See also *Fornaris* v. *Ridge Tool Co.*, *ante*, p. 41 (1970).

It is no answer to contend that there is no ambiguity in the Wisconsin statute and hence no need to abstain; in *Reetz* the Alaska statute could not have been more plain, or less susceptible of a limiting construction. Yet, in furtherance of this Court's firm policy to steer around head-on collisions with the States by avoiding unnecessary constitutional decisions, we reversed the District Court and remanded with instructions to stay its hand while the litigants exhausted state court remedies for resolution of their challenge to the statute. See also *Fornaris* v. *Ridge Tool Co.*, *supra*. *Reetz* cannot be distinguished and I see no reason to depart from the principles it reaffirmed.[2]

---

[2] Here there is not the urgency presented by *Reetz* where our action in remanding for state court consideration effectively precluded appellees from securing a commercial fishing license for at least one more season. No such urgency is presented by the instant case.

I quite agree that there is no absolute duty to abstain—to stay our hand—until the state courts have at least been asked to construe their own statute, but for me it is the negation of sound judicial administration—and an unwarranted use of a limited judicial resource—to impose this kind of case on a three-judge federal district court, and then, by direct appeal, on this Court. Indeed, in my view, a three-judge district court would be well advised in cases such as this, involving no urgency or question of large import, to decline to act.

This Court has an abundance of important work to do, which, if it is to be done well, should not be subject to the added pressures of non-urgent state cases which the state courts have never been called on to resolve. Neither the historic role of this Court nor any reasonable duty placed on us, calls for our direct intervention when no reason for expedited review is shown. Here we have an example of an unwise statute making direct review *prima facie* available, and an unwillingness by the Court to follow its own precedents by declining to pass on the Wisconsin statute before Wisconsin courts do so. We should remand this case with directions to the three-judge court to refrain from acting until the Wisconsin courts have acted.

MR. JUSTICE BLACK, with whom MR. JUSTICE BLACKMUN joins, dissenting.

I agree substantially with the dissent of THE CHIEF JUSTICE. I would vacate the District Court's judgment and remand with directions to withhold its proceedings to enable appellee to file a declaratory judgment or other state court action challenging the police chief's posting of notices in all Hartford retail liquor outlets forbidding sales or gifts of liquors to appellee for one year. As the Court's opinion, the cases there cited, and THE CHIEF JUSTICE's dissent point out, such a course of action is justified "where the issue of state law is uncertain" and where the state court might confine the state law's

meaning so "as not to have any constitutional infirmity." The Wisconsin Act appears on its face to grant authority to a man's wife, a mayor, a town's supervisors, the county superintendent of the poor, a sheriff, or a district attorney to post notices forbidding liquor establishments from giving or selling any alcoholic beverages to the person so posted. The effect of such sweeping powers, if there is nothing else in the State's law to limit them, is practically the same as that of an old common law bill of attainder, against which our forebears had such an abhorrence that they forbade it in Art. I, § 9, of the Constitution. See, *e. g.*, *United States* v. *Lovett*, 328 U. S. 303 (1946). And here the Wisconsin law purports on its face to place such arbitrary and tyrannical power in the hands of minor officers and others that these modern bills of attainder can be issued *ex parte*, without notice or hearing of any kind or character. It is impossible for me to believe that the Supreme Court of Wisconsin would uphold any such boundless power over the lives and liberties of its citizens. It seems to me therefore wholly uncertain that the state law has the meaning it purports to have, and I believe it is unfair to Wisconsin to permit its courts to be denied the opportunity of confining this law within its proper limits if it could be shown that there are other state law provisions that could provide such boundaries. For example, notice and hearing might be provided by principles of state administrative procedure law similar to the federal Administrative Procedure Act.

I realize that there are many cases where federal courts should not stay their hands to permit state courts to interpret state law. Compare *Clay* v. *Sun Insurance Office*, 363 U. S. 207, 213–227 (1960) (BLACK, J., dissenting), with *Burford* v. *Sun Oil Co.*, 319 U. S. 315 (1943). Here, however, no state court appears to have passed on this Act at all, and a state decision might well apply the body of other state law to require notice, hearing, and other necessary provisions to render the challenged Act constitutional.

JUDICIAL DECISIONS

OCTOBER TERM, 1970

May 24, 1971 (402 U.S. 1000)

No. 6106. TARVER *v.* SMITH, SECRETARY OF DEPARTMENT OF SOCIAL AND HEALTH SERVICES OF WASHINGTON. Sup. Ct. Wash. Certiorari denied. MR. JUSTICE BRENNAN is of the opinion that certiorari should be granted. Reported below: —— Wash. 2d ——, 470 P. 2d 172. [For earlier order herein, see 401 U. S. 906.]

MR. JUSTICE DOUGLAS, dissenting.

The ability of the Government and private agencies to gather, retain, and catalogue information on anyone for their unfettered use raises problems concerning the privacy and dignity of individuals.[1] Public and private agencies are storing more and more data. "If your name is not in the records of at least one credit bureau, it doesn't mean that you don't rate. What it does mean is that you are either under twenty-one or dead." [2]

A file may show that an individual was arrested. But will it show the arrest was unconstitutional because it was solely for purposes of investigation? Or that the charges were dropped? Or that a jury acquitted him?

Other "facts" may be in a file. Did he vote for Henry Wallace? Was he cited by HUAC? Is he subversive? Did he ever belong to any subversive organizations?

Private files amass similar irrelevancies and subjective information. Is he well regarded in his neighborhood as to character and habits? Does he have domestic difficulties? Is he "slow" in paying his bills?

---

[1] Law reviews have been devoting increasing attention to the problem. Recently two total issues have been devoted to the legal problems. See 15 U. C. L. A. L. Rev. 1374 and 31 Law & Contemp. Prob. 251. See also Symposium: Computers, Data Banks, and Individual Privacy, 53 Minn. L. Rev. 211; Note, Privacy and Efficient Government: Proposals for a National Data Center, 82 Harv. L. Rev. 400; Freed, A Legal Structure for a National Medical Data Center, 49 B. U. L. Rev. 79; Miller, Personal Privacy in the Computer Age, 67 Mich. L. Rev. 1091.

[2] H. Black, Buy Now, Pay Later 37 (1961).

The problems of a computerized society [3] with large data banks are immense. Who should have access to the files on an individual? For what purposes should access be allowed? Should an individual be informed each time information is passed on to new parties? How long should information be retained? What mechanisms ought there be for correcting factual errors?

This case presents the latter issue. A caseworker has prepared a highly critical report on petitioner setting forth in detail factual allegations and accusing petitioner of child neglect. The report recommends petitioner be permanently deprived of the custody of her children. Custody was temporarily placed in juvenile court because petitioner was hospitalized. Subsequently a hearing in juvenile court was held and petitioner was exonerated and retained custody of her children. But the critical report—which petitioner alleges is false—remains in the files with the Department of Social and Health Services of the State of Washington.

Not surprisingly, petitioner would like the allegedly false information removed from those files. But her efforts to obtain a hearing to correct the information have failed.

The State says that petitioner's file is "confidential and privileged" and under current state law the file may be disclosed only "for purposes directly connected with the administration of public assistance and specific investigatory purposes by legislative committees and properly authorized bodies." Respondent's Brief 6. Just how many people and agencies this includes is unclear. The only thing perfectly clear from this record is that

[3] "[T]he computer can also be an agent of oppression, if, for example, its fantastic memory is used to place indelibly on record all the events in a man's life, all his mistakes and weaknesses, precluding all hope of their effacement, every stimulating possibility of a new chance in life." R. Prebisch, Change and Development, Latin America's Great Task 209 (1970).

petitioner has no rights under state law to a hearing to correct the reports even if they are total lies. And it appears petitioner will never be informed prior to transmittal of her file to the various "authorized" groups.

The State contends that petitioner will suffer no harm from having the material in her files. We are told everyone will know the report is only an opinion; the decree of the juvenile court will be included; and the file will be treated confidentially. While, of course, we cannot know if the information is false and cannot tell which and how many uses will be made of the file, it is apparent that petitioner does raise some serious questions concerning its use. Participation "in the new Work-Incentive Programs is initiated by a referral by respondent's department of, among others, persons who are 'appropriate for referral.' R. C. W. 74.22.020; 74.23.040. Those who are referred receive substantial training benefits as well as increased cash benefits. R. C. W. 74.22.050, 060; R. C. W. 74.23.060, 070. Similarly, the availability of sheltered workshop programs depends upon a determination by the respondent's department that the subject, if a 'disadvantaged person,' 'can reasonably be expected to benefit from, or in his best interests reasonably requires' such a program. R. C. W. 28A.10.080 (2)." Petition 7 n. 2. The only answer that respondent gives to this is that any "information transmitted to the Employment Security Department under the Work Incentive Program is for the benefit of the recipient." How petitioner would benefit from the transmission of the allegedly false material we are not told.

The Washington State public assistance programs are designed to receive federal assistance whenever federal funds are available. Various provisions in the appropriate title of the Revised Code of Washington dealing with public assistance refer to conformity with and pri-

macy of federal law. *E. g.*, Wash. Rev. Code § 74.04.055 (Supp. 1970) (if more than one construction possible, favor that "most likely to satisfy federal laws"); Wash. Rev. Code § 74.23.005 (Supp. 1970) ("The legislature hereby expresses its intention to comply with the requirements under the federal social security act, as amended, creating a work incentive program" for mothers receiving Aid to Families with Dependent Children); Wash. Rev. Code § 74.23.900 (Supp. 1970) (if any part of the chapter conflicts with federal law it is to that extent inoperative). The record in this case is not clear as to which types of public assistance petitioner is receiving. Prior to the temporary unsuccessful attempt to remove her children from her custody she was receiving AFDC benefits. From the references in the briefs to eligibility for the AFDC Work Incentive Program it would appear that she is now again receiving AFDC benefits.

When federal funds are used, then standards are to be shaped and tested federally. *Helvering* v. *Davis*, 301 U. S. 619; *Ivanhoe Irrig. Dist.* v. *McCracken*, 357 U. S. 275, 295; *Rosado* v. *Wyman*, 397 U. S. 397, 427 (concurring opinion).

If meanwhile she was denied a fair hearing under state law, an important question of procedural due process is raised under the Fourteenth Amendment. For petitioner's right to continued assistance—an important property interest—cannot be reduced or terminated without notice and an opportunity to be heard. Cf. *Sniadach* v. *Family Finance Corp.*, 395 U. S. 337.

If petitioner was at the time receiving federal assistance then under HEW Regulations, she was entitled to a fair hearing.

The Department's regulations require that provision be made for granting a fair hearing:

> "to any individual requesting a hearing because his claim for financial or medical assistance is de-

nied, or is not acted upon with reasonable promptness, *or because he is aggrieved by any other agency action affecting receipt, suspension, reduction, or termination of such assistance or by agency policy as it affects his situation.*" 45 CFR § 205.10 (a)(3), eff. April 14, 1971 (emphasis added). 36 Fed. Reg. 3034.

As the Solicitor General says in his brief, filed at our request:

> "One may say, quite simply, that the report which petitioner challenges threatens receipt of AFDC payments by threatening to deprive petitioner of her children, on which her receipt of AFDC benefits depends. One of the federal requirements for a state plan for AFDC is that it must:
>
> "(16) provide that where the State agency has reason to believe that the home in which a relative and child receiving aid reside is unsuitable for the child because of the neglect, abuse, or exploitation of such child it shall bring such condition to the attention of the appropriate court or law enforcement agencies in the State, providing such data with respect to the situation it may have [42 U. S. C. (Supp. IV) 602 (a)(16)].
>
> "If any question were now to arise as to the suitability of the home for the children, the prior report might well have an effect on referral of the case to the courts and action by the courts, notwithstanding the 1967 decision of the Juvenile Court. Thus, the report retains a constant potential effect on petitioner's custody of her children and thereby on her receipt of assistance."

We cannot be sure of the exact posture of this case;

but whether or not the claim at the time was federally funded, a question of national importance is presented. Accordingly, I would grant the petition for certiorari.

CONGRESSIONAL RECORD EXCERPTS CONTAINING REMARKS ON PRIVACY BY MEMBERS OF CONGRESS

[From the Congressional Record, Senate, June 11, 1974]

NOTICE OF JOINT LEGISLATIVE HEARINGS ON PRIVACY AND GOVERNMENT INFORMATION SYSTEMS

Mr. ERVIN. Mr. President, hearings on bills relating to privacy and Government information systems will be held before an ad hoc subcommittee of the Senate Government Operations Committee and the Judiciary Subcommittee on Constitutional Rights on June 18, 19, and 20. The joint hearings will be held in room 3302 of the Dirksen Senate Office Building at 10 a.m.

The legislation before the Government Operations Committee is S. 3418, which I have cosponsored with Senators Percy and Muskie, to establish an administrative structure to oversee rules for the gathering and disclosure of information concerning individuals, and to provide management systems in Federal agencies, State and local governments and other organizations concerning such information, and for other purposes.

Bills pending before the Constitutional Rights Subcommittee of which I am also chairman, are: S. 2810, introduced by Senator Goldwater, to protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, V, IX, X, and XIV of the U.S. Constitution;

S. 2542, introduced by Senator Bayh to protect the constitutional right of privacy of those individuals concerning whom certain records are maintained; and

S. 3116, introduced by Senator Hatfield, to protect the individual's right to privacy by prohibiting the sale or distribution of certain information.

With these legislative hearings, the Government Operations Committee will continue its oversight of the development and uses of automatic data processing in the Federal Government. The intergovernmental nature of nationwide systems involving electronic and manual transmission, sharing and distribution of data about citizens has significant implications for our federal system. In its attempt to respond to citizens' demands for quality and quantity in services, government and the private sector have turned to the large data banks, computerized information systems and management techniques which will help them get the job done. Where these practices and systems neglect the administrative and technical concern for privacy, due process, and surveillance over the individual, they are taking a toll, which is yet unmeasured, on constitutional principles of accountability, responsibility and limited government. The cost to the taxpayer in dollars and cents concerns every American, for in the interest of promoting efficient government, the taxpayer may also be paying for loss of his privacy. That may be the price of insufficient monitoring by the public and Congress of the haphazard, ad hoc, ways modern government has found to meet its information needs, and which public officials use to meet their political needs.

Two Subcommittees of the Government Operations Committee are presently conducting oversight into major aspects of this problem. For instance, the Permanent Subcommittee on Investigations, chaired by Senator Jackson, is presently conducting an inquiry into surveillance practices in and out of government, including government wiretapping, eavesdropping, recording, industrial espionage and bugging of labor negotiations, and other monitoring practices.

The Intergovernment Relations Subcommittee chaired by Senator Muskie, who is also a sponsor of the pending bill, is considering legislation concerning electronic surveillance and the need to reorganize departments and agencies

37-583—74—pt. 2——19

engaging in such practices. That subcommittee is also studying a major aspect of Federal administration which affects individual privacy; this is the classification of Federal records and the laws and rules governing access, release and withholding of information which government collects about people.

The sponsors have introduced S. 3418 for purposes of discussion on the issues of what standards Congress should set for the protection of privacy in the development and management of Federal information systems, especially those which have been computerized with capacity for the sharing of records among departments and governments and across State boundaries. I expect hearings to produce expert advice not only on the standards to be set, but on the scope of the bill and how far the law should affect State, local, and private data banks. The hearings will also help us determine what kind of Federal structure should be established to enforce or advise on standards.

Congress is now considering a number of legislative proposals directed to specific problem areas of the law governing the privacy of the individual such as criminal justice data banks, military surveillance of civilian politics, wiretapping and eavesdropping, private credit data banks, employee privacy, behavior modification, lie detectors, and computer technology. These are some of the techniques and governmental programs which have concerned Congress and the public.

In contrast to such special legislation, the proposals considered in the June hearings represent general legislation to protect the privacy of all citizens and to build into the structure and practices of government a strengthened respect for the privacy and other freedoms guaranteed by the Bill of Rights.

S. 3418 is similar, but not identical, to omnibus legislation introduced by Representatives Edward Koch and Barry Goldwater, Jr., which is being considered by the House Government Operations Subcommittee on Foreign Operations and Government Information chaired by Representative William Moorhead. Their joint efforts are contributing greatly to the chances for enactment of major privacy protections this year. Individually, many Members of the House of Representatives have for a number of years sponsored bills reflecting sections of this proposal relating to mailing lists, a Federal privacy board, Federal questionnaires, and changes in the freedom of information law.

Portions of S. 3418 are similar to the measures pending before the Constitutional Rights Subcommittee. Another portion is comparable to my bill S. 1791 of the 91st Congress, which was to limit the threats to privacy from burdensome, overly personal questionnaires by which Government agencies sought statistical information through coercive collection techniques.

S. 3418 and the related bills deal with requirements to reveal one's social security number to government and private organizations, with personal statistical questionnaires, mailing lists, and remedies for official information programs which may pass constitutional boundaries.

In addition to the thousands of complaints which people have sent to Congress, we now have for guidance on this subject the investigative hearings, reports, and findings of a number of congressional committees, private organizations and Government departments. One of these studies, "Records, Computers and Rights of Citizens," was ordered by the former Secretary of Health, Education, and Welfare, Elliot Richardson, who will testify on June 18 on the findings of his study and the need for congressional and administrative action.

Another influential and comprehensive report entitled "Privacy and Freedom" by the Association of the Bar of the City of New York was directed by Prof. Alan F. Westin of Columbia University. Recently, Dr. Westin conducted another study with Michael F. Baker for the National Academy of Sciences entitled "Databanks in a Free Society." I am pleased to announce that in addition to presenting testimony on the pending legislation, Dr. Westin has agreed to serve as a consultant to our our hearings and to give us the benefits of his considerable research and analysis in this area of the law.

With the establishment of the new Domestic Council Committee on Right to Privacy chaired by the Vice President, Congress now has additional resources and assistance in its efforts to protect privacy, and we look forward to their cooperation in our studies.

Vice President Ford has accepted an invitation to present a statement on June 19 which will be delivered by the committee's Executive Director, Mr. Philip Buchan.

Other witnesses with special knowledge in this area of the law and administration will include Members of Congress who have sponsored privacy legislation, representatives of the National Governors Conference, the National Legislative

Conference, the National Association for State Information Systems, Government Management Information Sciences, the National League of Cities, the U.S. Conference of Mayors, the American Civil Liberties Union, Liberty Lobby, public administration specialists, and other interested organizations and individuals.

The Subcommittee on Constitutional Rights conducted excellent hearings in March of this year on criminal justice data bank legislation, in 1971 on "Federal Data Banks, Computers and the Bill of Rights," and in 1969 on "Privacy the Census and Federal Questionnaires." These hearings elicited for Congress a wealth of information about public complaints and attitudes concerning the establishment and the management of Federal programs to investigate citizens in order to store, distribute, and exchange information about them. We found that some of these programs were none of the business of the Government and infringed totally or in part on constitutional freedoms. Other programs were meant to obtain the great amount of information which Congress must have to legislate wisely and which the executive branch must have in order to administer the laws properly. In some instances, however, it was charged that lawful programs went beyond their purpose in scope, and in some cases, that the lack of adequate control permitted unauthorized access to this Government information, or allowed its transfer and distribution to unauthorized persons and those who had no need for it in the performance of their duties.

It is a rare person who has escaped the quest of modern goverment for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that this is a bipartisan issue which effects people in all walks of life. The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual. Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make it necessary for Congress to reaffirm the principle of limited Government on behalf of freedom.

The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information.

They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.

They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a number of years.

The pending legislation represents a partial solution to these concerns. There are alternatives to some of the provisions. For instance, enforcement of the act and the advisory functions which are located in an independent privacy board might be relocated or distributed to the General Accounting Office and the courts. Furthermore, after receiving testimony the committee may want to alter the scope of the legislation.

I want to commend Senator Percy for his interest in this subject and his initiative in working with House sponsors to bring the legislation before the Government Operations Committee in connection with its oversight of the use of governmental data banks and computer technology, and its monitoring of surveillance practices throughout government which may threaten freedom.

I hope the joint efforts of the Senate Government Operations Committee and the Constitutional Rights Subcommittee, whose members and staff have great expertise in this area of the law, will result in enactment of the basic legislative guarantees which are needed if America is to face up to the computer age.

It should be noted that these pending bills follow patterns and raise issues similar to those in criminal justice legislation, S. 2963 and S. 2964, which I have cosponsored with the following Senators who include members of the Judiciary and Government Operations Committees: Senators Hruska, Mathias, Kennedy, Bayh, Tunney, Young, Brooke, Mansfield, Robert Byrd, Burdick, Roth, Hugh Scott, Thurmond, Fong, and Gurney.

We welcome suggestions and comments from Members of Congress and others with an interest in and knowledge about these matters. Those wishing to submit statements for the record should communicate with the Government Operations Committee, room 3306 of the Dirksen Office Building, Washington, D.C. 20510, telephone 225–7469.

In an article entitled "The First Amendment—A Living Thought in the Computer Age," from volume 4 of the Columbia Human Rights Review, 1972, I have described some of the many complaints which people have registered to the Constitutional Rights Subcommittee and to Members of Congress about attitudes and program of government which threaten the privacy guaranteed under the first amendment. At the conclusion of the article, there is suggested a seven-part legislative program to remedy these complaints, part of which is reflected in the pending legislation. Additional examples of questionable data banks have been revealed, many of them documented in the forthcoming report of the subcommittee's comprehensive survey of the laws and rules affecting individual privacy in Federal data banks and computerized information systems. These new revelations to Congress merely serve to reaffirm my conviction that early congressional action is needed to implement the Constitution.

[From Congressional Record, Vol. 117, No. 13, Feb. 8, 1971]

ANNOUNCEMENT OF HEARINGS ON COMPUTERS, DATA BANKS, AND THE BILL OF RIGHTS

Mr. ERVIN. Mr. President, I am pleased to announce that the Subcommittee on Constitutional Rights has now rescheduled hearings on Computers, Data Banks, and the Bill of Rights. These will commence on Tuesday, February 23 at 10 a.m., and will continue on February 24 and 25, March 2, 3, and 4 and March 9, 10, and 11. They will be held in room 318 of the Old Senate Office Building every day except March 2 when they will be in room 1202 of the New Senate Office Building.

The subcommittee had planned to conduct hearings last October to consider the effect on individual rights of Government data banks and computer information techniques. I outlined for the Senate the purpose and scope of the subcommittee's study on September 8, 1970.

Unfortunately, the pressure of the Senate business made it impossible for the subcommittee to conduct the hearings with the full attention this vital subject requires. For that reason they were postponed until this time.

It has become increasingly clear that unless we take command now of the new technology with all that it means in terms of substantive due process for the individual who is computerized, we may well discover some day that the machines stand above the laws. By then, it will make no difference who mans the systems or what political party makes use of them, for the pattern of mechanized surveillance will have become so institutionalized throughout our land that it may defeat the ingenuity of the God-given powers of man to alter our national course. "Liberty" will then sound only as a word in our history books, the lamented dream of our Founding Fathers.

It was with these concerns in mind that the subcommittee initiated its Government-wide survey and investigation of computers and data banks. The overall goal of our hearings and studies therefore is fourfold: To learn, first what Government data banks have been developed; second, how far they are already computerized or automated; third, what constitutional rights, if any, are affected by them; and, fourth, what overall legislative controls, if any, are required.

We shall hear experts in computer technology discuss for us the development and application of computer systems as they affect the constitutional rights of individuals and the uses of political power in the United States.

Leadoff witnesses on February 23 will be Prof. Arthur R. Miller of the University of Michigan Law School and author of "The Assault on Privacy," a comprehensive analysis of this problem just published this week. Others in the field of computer technology will include invited representatives of the computer industry, including on March 3, Robert Henderson, vice president of Honeywell Corp. and on February 23, an official of the International Business Machines Corp. Robert Bigelow, attorney and chairman of the Committee on Computers and Society of the Association of Computing Machinery, and professor of computer science Caxton C. Foster will testify on March 10.

A major State computerized information system will be discussed on March 10 by Dr. Robert Gallati, director of the New York State Identification and Intelligence System. Furthermore, in his capacity as chairman of the project SEARCH privacy committee, he will discuss a major and singular report on a proposed national Federal-State computerized information system under the auspices of the Department of Justice.

While much of the current controversy revolves around computerization of law-enforcement information systems and data banks on special groups, there are other data-banking devices which concern every American, for they are essential to the lives of millions. Two of these are the social security number and the driver's license. The complaints received by the subcommittee indicate that these are two major problem areas of privacy and confidentiality.

It is becoming all too clear that these are common means of computerizing individuals and thereby locating them, investigating them, monitoring their activities for many purposes, and possibly invading their privacy and violating the confidentiality of the personal records stored in government and private computers.

The Secretary of Health, Education, and Welfare, Elliot Richardson, has recently expressed his concern about this and reported that he is studying the possibility that the Social Security number may be too broadly used. In a letter to me on September 15, 1970, he states:

"Social Security numbers are currently being used throughout industry and government as a means of clearly identifying individuals and avoiding the confusion and mistakes which can arise when a number of individuals have common or similar names. These numbers provide a unique means of identification applicable to most individuals in the United States . . .: Despite . . . restrictions, the Department is concerned that if the Social Security number were used too broadly, such widespread use and dependence upon the number might lend itself to abuses of individual privacy. Because of this concern, the Social Security Administration is currently reviewing the policies governing the issuance, maintenance, and usage of the Social Security number."

The subcommittee has invited Secretary Richardson to discuss this study of the uses of the Social Security number on March 11, as well as the various data banks used or sponsored by his Department. An invitation has also been extended to Secretary of Transportation John Volpe to appear on March 11 and discuss the Department's computerized national data bank of driver's license holders. This system contains information on all Americans whose licenses have ever been revoked; denied, withdrawn or suspended for any purpose.

As a data program established and expanded by Congress, one of concern to all Americans, and one developed and used cooperatively by Federal, State, local, and private agencies, this system should provide a useful example of the benefits and problems created by computer technology within the federal system.

Mr. President, beyond the constitutional and legal issues presented by the impact and uses of computer technology, there is a more profound question confronting the country. This is the extent to which the new computer science and information management techniques equip politicians with rapid and efficient tools for programs which have political ramifications for our entire society. Instant blacklisting, rapid cross-country exchange of dossiers, million-name master indexes, and scientific surveillance can easily become the order of the political day in this era of systems analysis and applied scientific management techniques.

These are practices suggested by the scope of some present Federal programs and they go to the heart of the constitutional exercise of first-amendment freedoms for every person in our society.

Since the issues here are of momentous concern, I believe they merit the careful scrutiny of this subcommittee and the Senate. The hearings, therefore, have significance in several ways, for they look to the way the power of government will be exercised over the individual in decades to come—they look even to the fate of our liberty in this century.

The scbcommittee's concern has been particularly prompted by increasing public interest and complaints about unwarranted governmental invasion of personal privacy through official surveillance and note taking on the political and personal activities of citizens who have broken no laws.

I am reluctant to attribute unsavory political motives to these programs, but there is no doubt that they were human responses to political forces at work in our society and in our Government. These official monitoring actions have been undertaken in the pursuit of a number of high sounding Federal programs, worthy in their inception. But, because of their scope, they threaten in operation to become, and in some cases actually have grown to be, monsters of the laws, stalking the privacy and trampling the first-amendment rights of individual citizens.

For example, there are the so-called civil disturbance prevention programs of the Army and other military services which were believed to require surveillance over lawful political activities of civilians. There are all the other "counterintelligence" programs which, justified or not, the armed services believe require surveillance and compiling of dossiers on civilians. These military activities have been discussed at length as each new revelation is made by agents who conducted the surveillance.

To get to the bottom of these complaints and learn how widespread the practices are, who authorized them and why; whether or not they continue today and under what restrictions, the subcommittee will hear a number of former military intelligence employees and agents describe their surveillance of citizens. We have invited Mr. Christopher Pyle to testify on February 24. Mr. Pyle is a lawyer and political scientist who has written widely on his experiences and observations while serving in the Army Intelligence Command.

Other agents will include Ralph Stein, who served in the civil disturbance analysis division in the Counter-Intelligence Command at Fort Holabird.

John M. O'Brien, who reported his monitoring of law-abiding citizens including political figures in Illinois, will appear on February 24, 1971, and wil be accompanied by Alexander Polikoff, attorney for the plantiffs in the suit against the Army for unwarranted surveillance of citizens in Chicago.

On February 25, Prof. Morris Janowitz, chairman of the Sociology Department, University of Chicago, will discuss such issues as the impact on the military services of their involvement in activities beyond their jurisdiction.

A number of organizations and private citizens will also testify on February 25 about their experiences and reactions to such Government programs.

On March 2, 3, and 4 we shall hear representatives of the Secretary of Defense describe the programs of each of the armed services and component agencies of the Defense Department with respect to note taking and record keeping of the activities of civilians who have no dealings with the Department of Defense. In addition, they will report to us on the contents, purpose and maintenance of the Army Investigative Records Repository, a basically manual system which contains dossier and reports on over 7 million Americans who have had reason to deal with the Department of Defense for personnel, counterintelligence, criminal, or other purposes. Since this is another major information system which is significant for many Federal programs, I believe a study of the transfer, exchange, retention and use of records in it will guide the subcommittee in its analysis of other programs.

I hope the Defense Department witnesses will enlighten Congress in considerable detail on the reasons for the unprecedented reports of spying and surveillance on political figures and on political-active citizens. I hope that they will describe in considerable detail the administrative actions they have taken—

First. To prevent unconstitutional excesses of power in the future;

Second. To purge completely each of their information systems of any reports they may have improperly compiled on civilians, at least over the past 20 years;

Third. To rescind in each of the services the vaguely-worded directives and memoranda issued at all levels and the regulations purporting to authorize excessive grant of surveillance powers in matters beyond the proper interests of the military.

We hope also to discover from these witnesses who else in the Federal Government received and data-banked the information compiled by the Army and other services, and what has been done to review and—where necessary, to purge—the files of those agencies.

In this aspect of the subcommittee study, the basic question at issue is the power of the executive branch to monitor the activities of individuals when there is no probable cause to believe they have committed a crime. The largest segment of such persons will be the political dissidents of all shades of political opinion who disagree intellectually and actively with Government policies or who associate with those who do. This is not a new problem in Government. We have known political blacklists before. The efficiency with which it is done now makes it a vital constitutional problem as never before.

While I find myself at loggerheads with many of these Americans, both with respect to their ideas and with respect to the means used to express those ideas, the vitality of our political system and the first amendment rights of all of us now and in the future depend on the extent to which their rights are protected.

For this reason, the subcommittee has extended an invitation to the Attorney

General, as chief legal officer of the Government, to discuss for the Congress what constitutional power rests in the executive branch and its respective department heads to conduct surveillance over such persons and to enter them in Federal data banks of the Justice Department and other agencies of government.

I believe these hearings will better enable the public, the press, the Congress and executive branch officials to understand the needs and purposes of government and the constitutional limits in our society to uses of the power of that government. It is my hope that the hearings will help Members of Congress respond quickly and effectively to complaints of invasion of privacy and to propose and act upon any remedial legislation which is found necessary.

[From Congressional Record, Vol. 116, No. 155, Sept. 8, 1970]

ANNOUNCEMENT OF HEARINGS: FEDERAL DATA BANKS AND THE BILL OF RIGHTS

Mr. ERVIN. Mr. President, in recent months, with the discovery of each new Federal data bank and data system, public concern has increased that some of the Federal Government's collection, storage, and use of information about citizens may raise serious questions of individual privacy and constitutional rights.

The Constitutional Rights Subcommittee has received countless letters and telegrams from Members of Congress and from interested persons all over the United States, urging that hearings be scheduled to consider the total impact of some of these data programs on preservation of individual rights.

I wish to announce that, in response to these demands, the subcommittee has scheduled a new series of hearings on "Federal data banks and systems and the bill of rights." The first stage of the hearings will be held October 6, 7, and 8.

The subcommittee has already undertaken a survey of Federal data banks and automated data systems to determine what statutory and administrative controls are governing their growth and what rights and remedies are provided for the citizen. The analysis of the executive branch replies to that subcommittee questionnaire, together with the hearings held in the last session on "privacy and Federal questionnaires," and the hearings which begin in October, will assist Congress in determining the need for a new independent agency to control Federal data banks on behalf of the privacy and due process rights of citizens. It has been my conviction that such an agency is needed, along with new remedies in the courts and other corrective actions. I detailed the reasons for my belief in a Senate speech in November 1969.

The purpose of the hearings is: First, to learn what Government data banks have been developed; second, how far they are already computerized or automated; third, what constitutional rights, if any, are affected by them; and, fourth, what overall legislative controls, if any, are required.

Witnesses familiar with the constitutional and legal issues, as well as the practical problems raised by some current and proposed data programs will document these for the record. The Secretary of the Army and other representatives of the Defense Department have already been invited to attend the October hearings to describe how and why the Army and other armed services have collected and stored information on civilians, and to what extent the records have been automated for easy access and retrieval.

Prof. Arthur R. Miller of the University of Michigan Law School, author of a forthcoming book, "The Dossier Society: Personal Privacy in the Computer Age," has been invited to describe the state of the law governing information flow in our society and its relationship to legal rights. Another witness will be Christopher Pyle, an attorney and former Army intelligence officer, who has investigated the Army's civil disturbance data programs, and has written widely on the subject.

In later hearings, other representatives of the executive departments and agencies will be invited to respond to the complaints and fears which have been expressed by the public. They will be afforded the opportunity to explain exactly what their data programs on people involve, and how, if at all, the privacy, confidentiality and due process rights of the individuals are respected.

The subcommittee has received enthusiastic support from specialists in the computer sciences, in both the computer industry and in the academic community. We hope to receive the benefit of their expertise for our hearing record.

Mr. President, our Nation is predicated on the fundamental proposition that citizens have a right to express their views on the wisdom and course of governmental policies. This involves more than the currently popular notion of a so-called right to dissent. Our system cannot survive if citizen participation is limited merely to registering disagreement with official policy; the policies themselves must be the product of the people's views. The protection and encouragement of such participation is a principal purpose of the first amendment.

More than at any other time in our history, people are actively expressing themselves on public questions and seeking to participate more directly in the formulation of policy. Mass media have made it easy for large numbers of people to organize and express their views in written and oral fashion. Rapid means of transportation have aided our mobile population to move easily to sites of central and local authority for the purpose of expressing their views more publicly. The freedom of our form of government and the richness of our economy have made it possible for individuals to move about freely and to seek their best interests as they will in vocations and avocations of their choice, or indeed, to pursue none at all for a time, if that is what they wish. If modern technology has provided citizens with more efficient means for recording their dissent, or for registering their political, economic, or social views, it has also placed in the hands of executive branch officials new methods of taking note of that expression of views and that political activity. For these reasons, those individuals who work actively for public causes are more visible than ever before.

These new sciences have accorded those who control government increased power to discover and record immutably the activities, thoughts and philosophy of an individual at any given moment of his life. That picture of the person is recorded forever, no matter how the person may change as time goes on. Every person's past thus becomes an inescapable part of his present and future. The computer never forgets.

To be sure, recordkeeping is nothing new in the history of government; nor indeed, is the habit all governments and all societies have of surveillance, blacklisting and subtle reprisal for unpopular political or social views. Men have aways had to contend with the memories of other men. In the United States, however, we are blessed with a Constitution which provides for due process of law. This applies to the arbitrary use of the recordkeeping and information power of government against the individual.

Despite these guarantees, the new technology has been quietly, but steadily, endowing officials with the unprecedented political power which accompanies computers and data banks and scientific techniques of managing information. It has given Government the power to take note of anything, whether it be right or wrong, relevant to any purpose or not, and to retain it forever. Unfortunately, this revolution is coming about under outdated laws and executive orders governing the recordkeeping and the concepts of privacy and confidentiality relevant to an earlier time.

These developments are particularly significant in their effect on the first amendment to our Constitution.

No longer can a man march with a sign down Pennsylvania Avenue and then return to his hometown, his identity forgotten, if not his cause.

No longer does the memory of the authorship of a political article fade as the pages of his rhetoric yellow and crumble with time.

No longer are the flamboyant words exchanged in debate allowed to echo into the past and lose their relevance with the issue of the moment which prompted them.

No longer can a man be assured of his enjoyment of the harvest of wisdom and maturity which comes with age, when the indiscretions of youth, if noticed at all, are spread about in forgotten file cabinets in basement archives.

Instead, today, his activities are recorded in computers or data banks, or if not, they may well be a part of a great investigative index.

Some examples come readily to mind from the subcommittee survey.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2,120,000 index cards. These bear lead information relating to possible questions of suitability involving loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II. The Commission has found it a reasonable, economical and invaluable tool in meeting its investigative

responsibilities. It is usful to all Federal agencies as an mportant source of information.

The Commission chairman reports:

"Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting."

In its "security investigation index," the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigatons made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

The Commission's "investigative file" consists of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

For authorization for these data banks, the Commission cites Executive Order 10450, an order promulgated in 1953.

Another department, the Housing and Urban Development Department, is considering automation of a departmental procedure. According to the report made to the subcommittee:

"The data base would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File. A data bank consisting of approximately 325,000 3x5 index cards has been prepared covering any individual or firm which was the subject of, or mentioned prominently in any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well. In addition, HUD maintains an index file on all Department employees which reflects dates and types of personnel security investigations conducted under the provisions of Executive Order 10450."

In the interest of preparing for possible civil disturbances and for protecting the armed services from subversion, the Department of the Army and other military departments have been collecting information about civilians who have no dealing with the military services.

The Secret Service has created a computerized data bank in the pursuit of its programs to protect high Government officials from harm and Federal buildings from damage. Their guidelines for inclusion of citizens in this data bank refer to "information on professional gate crashers; information regarding civil disturbances; information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas; information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, and so forth."

In this area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs. The initial data base, according to the Secretary of the Treasury, is a "modest" one comprising some 3,000 suspect records: He states:

"These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and usable form. With the coordinated efforts of the Agency's Service's intelligence activities, steady growth of the suspect files is expected."

This data bank, which is used by the Bureau to identify suspect persons and vehicles entering the United States, is an "essential tool" in performance of Customs officers' search and seizure authority, Secretary Kennedy has stated.

The Department of Justice is establishing comprehensive law enforcement data systems in cooperation with State governments, and is funding State data programs for law enforcement, civil disturbance and other surveillance purposes.

The National Science Foundation has created a data bank of scientists.

The Department of Health, Education, and Welfare has established a data bank on migrant children to facilitate the transfer of school records.

During our subcommittee hearings last year, case after case was documented of the vast programs to coerce citizens into supplying personal information for statistical data banks in the Census Bureau and throughout other Federal agencies.

These are only a few of the data programs which have raised due process of law questions from Congress and the public.

How do these things come about? It would be unfair, perhaps, to attribute suspicious political motives, or lack of ethics to those responsible for any one program or for any group of programs for collecting and storing personal information about citizens. Frequently, they just grow over the years. Sometimes, executive department data banks are either merely good faith efforts at fulfillment of specific mandates from Congress; or they are based on what some officials think to be implied mandates to acquire information necessary for Congress to legislate. If so, then Congress has no one to blame but itself when such programs unnecessarily threaten privacy or other rights. But it then has an even greater responsibility for acting, once its own negligence is discovered.

Perhaps the most such officials can be charged with is overzealousness in doing their job within narrow confines, to the exclusion of all other considerations.

Sometimes the issue of threats to individual rights is presented only after a data system has developed, and only after practical problems are raised which were not envisioned on paper.

At times, due process may be threatened by the failure of the computer specialists to consider only the information on a person absolutely essential for their programing.

There are political reasons also. One is the failure of heads of executive departments and agencies to mind their own stores and stay out of the business of other agencies. Each department does not need to seize the total man when it administers a program; only those portions of him necessary for the job. Another reason is the tendency of executive branch officials in the interest of political expendiency and shortcuts to law and order goals, to seize upon the techniques of data banks, intelligence gathering, and surveillance activities as a substitute for hard-hitting, practical law enforcement work by the proper agencies, and for creative administration of the laws.

All of these excuses will not help the law-abiding citizen who, at the whim of some official, is put into an intelligence-type data bank which is part of a network of inquiry for all manner of governmental purposes.

No one would deny that the Government of such a populous and farflung country should not avail itself of the efficiency offered by computers and scientific data management techniques. Clearly, Government agencies must, as Congress has charged them, acquire, store, and process economically the information it obtains from citizens for administrative purposes. There is an ever-increasing need for information of all kinds to enable the Congress to legislate effectively and the executive branch to administer the laws properly.

Furthermore, there is an obvious need in such a complex mobile society for recording and documenting amply the official relationship between the individual and his government.

More and more frequently, misguided individuals are resorting to violence and violation of the law. Communities are faced with rising crime rates. Local, State, and Federal Government have a right and a duty to know when a person has a legal record of violation of the law which, under the law, would deny him certain rights or benefits. They should be able to ascertain these matters quickly.

There are always some problems of accuracy and confidentiality with such records, especially when automated. It is not the carefully designed individual law enforcement data banks which concern the public. Rather, the subcommittee study is revealing that data programs which have aroused the most apprehension recently are those—

Which bear on the quality of first amendment freedoms by prying into those protected areas of an individual's personality, life, habits, beliefs, and legal activities which should be none of the business of Government even in good causes;

Which are unauthorized, or unwarranted for the legitimate purpose of the agency;

Which keep the information they acquire too long, and which by the very retention of unknown data may intimidate the individual subject;

Which are part of a network of data systems;

Which make little, if any provision for assuring due process for the individual in terms of accuracy, fairness, review, and proper use of data, and thereby may operate to deny the individual rights, benefits, privileges, reputation, which are within the power of government to influence, grant or deny.

There is growing concern that the zeal of computer technicians, of the systems planners, and of the political administrators in charge of the data systems threat-

ens to curtail the forces of society which have operated throughout our history to cool political passions and to make our form of government viable by allowing a free exchange in the market place of ideas.

The new technology has made it literally impossible for a man to start again in our society. It has removed the quality of mercy from our institutions by making it impossible to forget, to forgive, to understand, to tolerate. When it is used to intimidate and to inhibit the individual in his freedom of movement, associations, or expression of ideas within the law, the new technology provides the means for the worst sort of tyranny. Those who so misuse it to augment their own power break faith with those founders of our Constitution who, like Thomas Jefferson, swore upon the altar of God eternal hostility against every form of tyranny over the mind of man.

Mr. President, it has become dangerously clear in recent times that unless new controls are enacted, new legal remedies are provided, and unless Federal officials can be persuaded to exercise more political self-control, this country will not reap the blessings of man's creative spirit which is reflected in computed technology. Rather, if the surveillance it encourages is allowed to continue without strict controls and safeguards, we stand to lose the spiritual and intellectual liberty of the individual which have been so carefully nourished and so valiantly defended, and which our Founding Fathers so meticulously enshrined in the Constitution.

I say this out of my conviction that the undisputed and unlimited possession of the resources to build and operate data banks on individuals, and to make decisions about people with the aid of computers and electronic data systems, is fast securing to executive branch officials a political power which the authors of the Constitution never meant any one group of men to have over all others. It threatens to unsettle forever the balance of power established by our Federal Constitution.

Our form of government is the fruition of an ideal of political, economic, and spiritual freedom which is firmly rooted in our historical experience. Basic to its fulfillment has always been the monumental truth that such freedom is truly secure only when power is divided, limited, and called to account by the people. For this reason the central Government was divided into three separate and equal branches.

For this reason, the bill of rights was added to secure certain areas of liberty against incursion by Government and the exercise of Federal power was limited to certain purposes.

For this reason, we cherish and protect the legal freedom of each citizen to develop his mind and personality and to express them free of unwarranted governmental control.

I differ with those who say that there are no existing checks on this developing power of computer technology, for I believe they already exist in our form of Government. The guarantees are established in our Constitution.

The forthcoming hearings will help Congress determine how these guarantees may best be implemented to meet the demands of the computer age.

In the interest of responding to the many inquiries from scholars, reporters and members of the public who are working on this subject, I should like to refer to other sources of materials which provide useful background information.

The subject of how Government manages its information systems, and its paper work, how and when it uses computers and automation to assist in this effort, has been a continuing subject of concern by a number of congressional committees and their efforts should interest those working on this subject.

The Senate Administrative Practice and Procedures Subcommittee has contributed valuable hearings, reports and studies on the subject of computers, privacy, and Government dossiers. Particularly informative in their 1967 report "Government Dossier: Survey of Information on Individuals Contained in Government Files."

The Senate Government Operations Committee has, in other years, conducted comprehensive hearings and issued reports on Government information systems and management uses of computers.

In the House of Representatives, the Committee on Science and Astronautics has held a provocative and stimulating series of hearings and panel discussions on the impact of technology, especially on the management of Government information.

The House Government Activities Subcommittee of the Government Operations Committee, chaired by Representative Jack Brooks, has produced valuable

hearings, reports and legislation on "Data Processing Management in the Federal Government."

More than anyone else, Representative Cornelius Gallagher has continually pointed out the dangers to individual rights and privacy of the establishment of a national data center, and his Special Subcommittee on Invasion of Privacy, after stimulating hearings, produced a classic and concise report entitled, "The Data Bank Concept." The record of his hearings contains testimony from many expert witnesses on the philosophy of privacy and computer technology.

The Census and Statistics Subcommittee of the House Post Office and Civil Service Committee produced a thought-provoking and influential report in the 89th Congress entitled "The Federal Paperwork Jungle." Scholars will find most informative that subcommittee's hearings and reports dealing with the paperwork requirements placed upon business, industry, and the public by the Federal departments.

I commend the publications of all of these committees and the thoughtful speeches of the chairmen and the members of these committees to persons interested in this subject.

It is my hope that the hearings and study by the Constitutional Rights Subcommittee will add a unique and valuable dimension ot the public and congressional dialog on the role of data banks, information systems, and computers in our constitutional form of government.

[From the Congressional Record, Nov. 10, 1969]

COMPUTERS AND INDIVIDUAL PRIVACY

Mr. ERVIN. Mr. President, last week I attended a conference of management executives at the Wharton School of Finance and Commerce, University of Pennsylvania. These executives were discussing the science and management of information systems. The Constitutional Rights Subcommittee, in the course of its investigation of Government invasion of privacy, has uncovered many violations of the personal privacy of Federal employees and applicants. Many of these were made possible by the creation of vast computerized data banks. It was for this reason that I introduced S. 782, the right-to-privacy bill, which 54 Members of the Senate have cosponsored. As the complaint from Federal employees and every major employee union and organization demonstrate, there is an urgent need for enactment of this legislation.

Millions of private citizens face similar surveillance by computers in private industry as well as in Government. Their problems are equally deserving of attention.

Due to the national dimensions of this problem and its complicated nature, it is well-nigh impossible for Congress, by any one law, to control the danger posed to our society by computer technology.

For this reason, in addition to bills prohibiting the collection and use of Federal data on individuals, there is an immediate need for establishment of an independent regulatory agency to control this new communication-surveillance system.

I also discussed at the conference a striking example of the dangers which Federal data banks present to individual privacy. This is a guideline published by the Secret Service and distributed to Federal employees to encourage them to report on private citizens. I have asked the Secretary of the Treasury to report to the subcommittee about the methods of compiling and using this data, for preserving its confidentiality, and for notifying citizens that a report has been made and affording a chance for rebuttal.

I ask unanimous consent that there be printed at the conclusion of my remarks my letter on behalf of the subcommittee to Treasury Secretary David M. Kennedy together with a letter to the Commission of Internal Revenue from the American Civil Liberties Union which was supplied to the subcommittee with the Commissioner's response.

The PRESIDING OFFICER. Without objection, it is so ordered.

(See exhibit 1.)

Mr. ERVIN. Mr. President, the conflict between the needs of our computer age and individual privacy in our national life is a problem which we used to think was uniquely American but technological know-how has made this a worldwide, and possibly, after Appollo 11, a universal concern.

From my investigation, I am convinced that computers represent a magnificent contribution to the progress of mankind. In fact, they are so wonderful that I considered introducing an amendment to allow a computer to be elected President. But I found that while it can make logical conclusions from information fed into it, it cannot draw illogical deductions from logical facts. For this reason, a computer could never be President and I didn't introduce my proposed amendment.

There is a common bond which unites most of the population today. All of us have been, or will be, victimized or harassed by a computer. Last year I received a check from the social security agency for $754.25 for lumpsum death benefits. I returned the check with a letter saying I was happy to report that contrary to the computer's deduction, any indications that I had passed away were slightly exaggerated.

Another time, when my income tax was not being withheld from my salary, I received a computerized notice from the Internal Revenue Service that I had failed to pay my June installment. I replied that this had been paid and eventually I learned that someone had failed to enter my payment in the computer.

So if the computer has, through folklore, acquired an image of infallibility, this is not the image it has in my mind.

Nor is the image in the minds of those countless millions of Americans whose reputations, jobs, credit and insurance ratings, health records, security clearances, driver's licenses, and Government benefits of many different kinds may be destroyed or threatened by a computer. These are the people who stand to suffer at some time in their lives from erroneous information in their computer files which they cannot confront or explain.

These are the people who are being denied, or will be denied, due process by medium-size businesses and large corporations, by organizations and by government at all levels. These are the people in every type of work and every walk of life who must fear the mechanical or human quirks or complete breakdowns in computerized information systems.

They are also the millions of citizens who will be harassed by overzealous computerized data-collecting programs of overcurious administrators; the people who will wonder what the form they filled out was all about, and what will be done with their replies.

The number of citizens whose privacy is affected is vast. A survey by the Senate Administration Practices Subcommittee 2 years ago revealed that—

Our names alone are in government files 2,800 million times. Our social security numbers are listed 1,500 million times. Police records number 264,500 million; medical histories, 342 million; and psychiatric histories, 279 million.

The social security number once was treated as a private matter, sacred to the individual. That was in the 1930's before the computer age. Now, with this number on almost every Government form, and every private questionnaire, no man can be lost. And this is reassuring. But, similarly, no man can ever again be alone. And this is despairing.

The new plan of the Health, Education, and Welfare Department to tie in a national welfare program to the social security system raises specters of surveillance and privacy invasion on a scale never before experienced. Only time will tell what the bureaucrats will do with this. Sadly enough, it will be the poor, the unsophisticated, the inexperienced, who will have to fight the computers in this program.

It is not just the chance of wrong or one-sided information being fed into vast Government and private computer systems that should give us cause to worry.

The increased use of computers makes it cheaper and vastly more simple for Government as well as private businesses to collect and store information about people for reasons that would give us serious pause.

There is, for instance, the Secret Service's well-meaning program to keep track of people who might harm the President or other public officials. But consider this Secret Service memorandum telling employees of Federal agencies to supply—

Information about individuals who "make oral or written statements about high Government officials in the following caegories"; Threatening statements; irrational statements; and abusive statements.

Information on professional gate crashers.

Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, and so forth.

Information pertaining to a threat, plan, or attempt by an individual, a group, or an organization to physically harm or embarrass the persons protected by the U.S. Secret Service, or any other high U.S. Government official at home or abroad.

Many people, with complete faith in their Government, believe that the place to start with a complaint is with the President or Vice President. Yet some of these people who write a strong letter will never know they have been fed into yet another Government data system. Are these records now to be part of standard employment checks for suitability and security clearances?

Another change made possible by the computer is that statistical questionnaires can now be distributed by private agencies and by Government in a scale beyond the researcher's wildest dreams. It has been estimated that by 1970 the total statistical budget of the Federal Government will probably exceed $200 million. If complaints to Congress are any indication, the impact on individual rights of these programs is proving devastating.

The decennial census questionnaire, with civil and criminal penalties, is one example of this, with such questions as:

How much rent do you pay?

Do you live in a one-family house?

Do you use gas?

If a woman, how many babies have you had? Not counting still births.

How much did you earn in 1967?

If married more than once, how did your first marriage end?

Do you have a clothes dryer?

Do you have a telephone, if so, what is the number?

Do you have a home food freezer?

Do you own a second home?

Does your TV set have UHF?

Do you have a flush toilet?

Do you have a bathtub or shower?

Another example of this computer prying occurred last spring when the Constitutional Rights Subcommittee began receiving complaints from elderly, disabled, or retired people in all walks of life about a 15-page form sent by the Census Bureau. It asked questions such as:

What have you been doing in the last 4 weeks to find work?

Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?

Do you have any artificial dentures?

Do you—or your spouse—see or telephone your parents as often as once a week?

What is the total number of gifts that you give to individuals per year?

How many different newspapers do you receive and buy regularly?

About how often do you go to a barber shop or beauty salon?

What were you doing most of last week?

When the recipient did not respond he received a second form by certified mail, then a phone call, and then a visit from a Census Bureau employee.

We found that because of its great computer systems, the Census Bureau was sending out this form for the Department of Health, Education, and Welfare. We also found that it was making similar surveys of many other groups such as the mentally ill and the handicapped. It took the subcommittee several months, several letters, and a number of phone calls to get an answer from the HEW Secretary to the simple question, whether or not this form was voluntary or required. We also found that several sets of tapes were made of the responses and stored in several different places: in one location, apparently forever.

As a result of those and thousands of other complaints about burdensome or privacy invading statistical forms, I had the Senate Constitutional Rights Subcommittee conduct a survey of every Federal agency to find out what kind of statistical questionnaires they are sending to the public, whether the replies were voluntary or required, and finally, whether the person who received the form was told this. We learned that over the past 3 years Census Bureau alone had conducted 87 voluntary surveys for 24 other agencies which covered over 6 million people. There were other independent surveys by the agencies themselves. Everything from bomb shelters to smoking habits, to birth control methods was included in these "people studies." And usually with spaces for social security number, address, and phone numbers on the form. All responses were fed into computers.

The Census Bureau and Health, Education, and Welfare questionnaires illustrate another serious problem basic to the computer age. The right to privacy and the right to keep silent about one's personal life and attitudes is being violated by the coercive methods used by government and business to obtain responses. The information fed into these machines is easliy coerced by citing a general statute or by using subtle psychology to pressure a response. The Assis-

tant Secretary of Commerce for Economic Affairs, William H. Chartner, for instance, told the subcommittee that he could not advise people that their responses to a form were voluntary because that would be "bad psychology." He felt that the Census Bureau had to give the citizens the impression his replies were required on pain of penalty.

We frequently see such pressure applied to applicants for employment who are forced to subject themselves to wholesale invasion of their personal privacy because they need a job. This is particularly true in private businesses. The data disappears into the labyrinth of computers, and as the person moves from job to job throughout an industry, the computer surveillance continues, facilitated by the network of interfacing computer systems.

Because there are few controls, the applicants and employees of these large corporations which stretch across our national economy are subjected to a startling arsenal of devices for coercing disclosure of personal information.

Do they want to check an applicant's capacity to fit into the organization—his conformity to the prevailing norm? They subject him to personality tests and make a record in the computer dossier of his responses to such questions as:

I am very seldom troubled by constipation.
My sex life is satisfactory.
At times I feel like swearing.
I have never been in trouble because of my sex behavior.
I do not always tell the truth.
I have not lived the right kind of life.
I have no difficulty in starting or holding my bowel movements.
I am very strongly attracted by members of my own sex.
I like poetry.
I go to church almost every week.
I believe in the second coming of Christ.
I believe in a life hereafter.
I loved my mother.
Many of my dreams are about sex matters.

Congress has received complaints about such psychological pressure from the practices of larger credit companies. With their gigantic computerized data systems, they induce the most personal revelations out of the individual through subtle threats or inducements of credit clearance. Yet his buying and borrowing ability is governed wherever he moves in this country or abroad by the rapid computer transmission of information about him.

As of now, however, the individual has no recourse, no chance of confronting and rebutting the data.

The forms of human psychology promoted by computer technology today are about on the same moral plane as false pretenses in a horse trade.

Whether practiced by private business or by government, they have no place in our constitutional system, and under American ideas of due process.

REMEDIES

What can be done about these threats to our liberties? How can we insure that corporations as well as Government afford substantial due process to employees and citizens?

Our Founding Fathers, with all their vision, could not have foreseen the "memory banks" and "printouts" that are beginning to dominate our society.

Our present legal system affords no protections against the excesses of computers, and no adequate legal remedies for the injuries they may cause. But under our Constitution, this can be remedied.

To mitigate, much less prevent these threats, there must be controls of several kinds.

First. There must be technical and mechanical security devices built into the machine. According to engineers, this is possible and the computer industry should be encouraged to develop these.

Second. There must be controls for those who operate and who control the machines. In this connection, the ethical conduct guidelines with some of the computer operators themselves have developed and are attempting to apply, suggest that the industry will try to police itself, will develop sanctions, and hopefully, publicize their use, for any personnel who violate its code. In addition, strict administrative personnel rules must be developed by organizations, businesses and industries using computers.

Third. To assure substantive due process, there must be controls over computer input and output. Since one of the most basic threats posed by the computer is the exchange of information among agencies and among companies, information collected for one purpose should not be utilized for another without tight conditions attached, without the involvement of the individual.

Fourth. Some system must be devised to give the individual a chance to explain personal data susceptible to derogatory interpretation. One of the drawbacks of our highly mobile, computerized society is that a man's past is ever with him. He should have a chance to expunge the record.

Walter Malone expressed the sentiment in his poem, "Opportunity":

"Weep not for precious chances passed away!
Weep not for golden ages on the wane!
Each night I burn the records of the day—
At sunrise every soul is born again!"

Yet the people most concerned with out growing communications—surveillance system are given no chance for due process. In many cases, the victim never knows why or how he has failed in an endeavor.

As Prof. Arthur R. Miller writes:

"The computer's impact on traditional relationships between individuals and organizations, and the impending emergence of computer technology as a medium of communication with national dimensions, suggests that congressional action to protect privacy values may be both necessary and appropriate."

However, I agree with Professor Miller that the uncertain direction of the computer age and the lack of obvious and easy solutions have combined to make the desirability and effectiveness of congressional action still very much a matter of conjecture. Furthermore, as he points out:

"Our limited experience with data centers and networks and the enormously complex problems of distinguishing between governmental and private systems and determining the extent to which the private ones should be federally regulated make the obstacles to drafting comprehensive national legislation virtually insurmountable at the present."

Fifth. The most effective action Congress can take is the enactment of laws controlling the collection and the use of data in certain areas. Examples of this are S. 782, my Federal employee privacy bill; S. 1791, my bill to limit certain types of privacy invasion by governmental statistical questionnaires; and proposals for some type of credit reporting act to protect consumers against erroneous credit reporting.

Sixth. If the problem of computer technology is too vast to be dealt with in one statute, still I believe it can be controlled by the Federal Government in the same way we have handled other vast, complex communication problems such as the radio, telegraph, television, and telephone. This is through an independent regulatory agency.

I see no existing agency which could assume these complicated and delicate problems. Those charged with regulating communications have built-in biases in their operating methods and their approaches to these problems, particularly the preservation of individual privacy.

While I dislike adding to an already weighty bureaucracy, the problem is serious enough to warrant a separate agency. For this reason, therefore, I would support the creation of some separate agency to deal specifically with computer systems.

I believe we have learned enough over the past 50 years about the design and operations and problems of regulatory agencies to enable us to create one which has built-in protections to assure that it serves the interests of the individual citizen and not solely those of the industry it is supposed to regulate.

Beyond the immediate legal and practical threats to individuals, there is a greater danger to our social fabric presented by the network of computer systems which crisscross the Nation. These mammoth communications devices, while encouraging actual surveillance, in certain circumstances under certain conditions, have also created a climate of apprehension and fear of "snoopers"—private or official.

To the alienated in our society, and to the not-so-alienated, the computer card either has become, or stands in danger of becoming, a symbol of administrative coldness, of dehumanized impersonal decisions lacking the input which ideally should inform administration in any organization with fairness, intelligence, and humanity.

The reasons for this growing public attitude should be carefully considered by executives in the public as well as private sector of our national life.

Seventh. On both sides, public and executive, there is a real need for education and for reassessment as to what corporate or governmental goals are important in this computer age.

Efficiency and economy can be balanced with privacy and constitutional freedom. But it must be done now if our form of liberty is to survive.

The computer field is so vast that talking about it is like the story of the two elderly ladies in a town in North Carolina. They entertained the new young preacher on Sunday afternoon, and then invited him to dinner that evening. He said he had to preach at Sunday evening service first, so one of the ladies stayed home to prepare the dinner and the other went with the preacher to the church. When they returned after the services, the one who had stayed home asked how he had preached. The other lady said he had preached in the apostolic style. He just took the gospel and preached all over the place.

That is what it is easy to do with the subject of computers. The implications and impact of computers on our society are almost inconceivable in their immensity and intensity. One can talk about the issue at great length and to great extent and never exhaust the subject, never completely resolve the problem.

While I believe that much more thought and discussion should be devoted to the legal and social implications of a computer-based civilization, I am not in favor of our merely preaching all over the place for the indefinite future. We know enough now of the implications of this technology to begin taking action both in the private and the public sectors to bring the electronic brains under effective control of the human beings they are created to serve.

EXHIBIT 1

NOVEMBER 10, 1969.

Hon. DAVID M. KENNEDY,
Secretary of the Treasury,
Washington, D.C.

DEAR MR. SECRETARY: In connection with the Constitutional Rights Subcommittee's study of data banks and individual privacy, I have been seriously concerned about the guidelines issued by the Secret Service to encourage federal employees' reporting on private citizens for a vast number of reasons. I discussed this last week in a speech on "Computers and Individual Privacy", a copy of which is enclosed for your use.

I have no quarrel with the goal of the Secret Service to perform their duties efficiently. It is clear, however, to anyone educated in our constitutional form of government, that the criteria for filing information about individuals are questionable from a due process standpoint; are impractical; and are conducive to a mass surveillance unprecedented in American history.

Your attention is directed to such examples in the guidelines as the invitation to Civil Service workers throughout government to supply:

1. Information about individuals who "make oral or written statements about high government officials in the following categories": (2) Threatening statements; (2) Irrational statements; and (3) Abusive statements.

2. Information on professional gate crashers.

3. Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.

4. Information pertaining to a threat, plan or attempt by an individual, a group, or an organization to physically harm or *embarrass* the persons protected by the U.S. Secret Service, or any other high U.S. Government official at home or abroad.

5. Information about people who take part in demonstrations.

These guidelines are a direct threat to first amendment freedoms.

Many people, with complete faith in their government, believe that the place to start with a complaint is with the President or Vice President. Yet some of these people who write a strong letter will never know they have been fed into yet another government data system. Similarly thousands of well-meaning, loyal Americans have engaged in some form of demonstration in connection with the Vietnam war, welfare and civil rights policies of the government, and many other causes.

What the Subcommittee wishes to know in order to respond to complaints about this surveillance is:

Are these records now to be part of standard employment checks for (a) suitability and (b) security clearances? What standards have been promulgated by

the Secret Service for maintaining such a data bank? Will this information be computerized? Will it be available for use by other federal agencies? If so, which ones?

What procedures have been established for (1) Preserving the confidentiality of this data; (2) affording citizens subject to such a report the opportunity to review their files and to rebut derogatory information?

Would you also supply copies of any published federal regulations governing this data bank and its use.

Your assistance in our study is appreciated.

With all kind wishes, I am.

Sincerely yours,

SAM J. ERVIN, Jr.,
Chairman.

AMERICAN CIVIL LIBERTIES UNION,
Washington, October 22, 1969.

Hon. RANDOLPH W. THROWER,
Commissioner, Internal Revenue Service, U.S. Treasury Department, Washington, D.C.

DEAR COMMISSIONER THROWER: A recent supplement to the Internal Revenue Service Manual regarding protection of the President entitled, "Guidelines for Reporting Information", dated August 26, 1969, has come to our attention. Recognizing as we do the importance of safeguarding the life of the President, nevertheless, it appears to us that a number of the guidelines contained in that supplement are overly broad and devoid of relevance for that purpose. They will succeed in doing nothing but adding to investigative files the names of American citizens who are doing nothing more than exercising their right of freedom of speech and their right to petition their government for redress of grievances. The disastrous effects of having information considered derogatory in such investigative files on employment possibilities, security clearance and even to positions on advisory committees of government agencies is too well known to require reiteration here. (You may have noticed recent news stories in the *New York Times* concerning scientists being blacklisted by HEW for service on advisory review committees on the basis of such so-called derogatory information.)

In particular, I would like to suggest modification be considered or elimination of the following guidelines:

I. PROTECTIVE INFORMATION

A. Information pertaining to a threat, plan or attempt by an individual, a group, or an organization to physically harm or *embarrass* the persons protected by the U.S. Secret Service, or any other high U.S. Government officials at home or abroad.

Comment: Certainly the desire to embarrass any government official hardly indicates a desire to harm him. Embarrassment may be caused in many ways, including the exposure of peccadilloes, or even malfeasance in office.

D. Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imiginary grievances, etc.

Comment: Many Americans attempt to contact high Government officials for the purpose of redressing grievances. The grievances may be in the view of some individuals including the government officials involved, imaginary. Nevertheless, it is fairly clear many of the grievances are not imaginary and it has only been by the sustained effort of such individuals that the grievances have been brought to public attention and corrective measures taken. American citizens should not be inhibited in trying to see high government officials by fear that this will be considered derogatory information by the Secret Service.

E. Information on any person who makes oral or written statements about high Government officials in the following categories: (1) threatening statements, (2) *irrational statements*, and (3) *abusive statements*.

Comment: A comment similar to the item above could be made about irrational statements and abusive statements. There are many people who write abusive letters and make abusive statements about government officials. However, merely because a letter or statement is abusive in tone does not indicate a desire to cause physical harm. Similarly, those who make irrational statements

do not necessarily indicate any desire nor inclination to harm. Unless the purpose of this guideline is really just to collect a list of all those who make abusive or irrational statements about high government officials in the United States, it seems difficult to believe that this kind of information is necessary as a positive method of protecting such officials.

Just in passing—the recent speech by Vice-President Spiro Agnew reported in yesterday's *Washington Post* and *New York Times* as well as being carried by all the news media, was considered by at least Senators William Fulbright and Hugh Scott to be abusive about some Congressional leaders who are opposed to the war in Vietnam. Would Vice President Agnew's speech be covered by this regulation and would it have to be reported?

I. Information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas.

Comment: To be specific, are the recent moratorium demonstrations on October 15th considered to be either anti-American or anti-Government and must all participants be reported to the Secret Service? If so, are you including the names of all the U.S. Senators and Congressmen who participated?

Is there a difference between anti-American or anti-U.S. Government or is one term intended to mean anti-administration?

As I stated at the beginning of my letter, I recognize the necessity for guarding the President and other government officials protected by the U.S. Secret Service. However, collecting information of the kinds suggested in these guidelines will not really focus on this problem and instead, will fill investigatory files with useless information which will be derogatory to countless millions of Americans.

We would appreciate your reconsidering this manual supplement. We would be quite willing to discuss this matter further either with you or with those who have the responsibility of issuing such instructions.

Sincerely yours,

LAWRENCE SPEISER,
Director, Washington Office.

INTERNAL REVENUE SERVICE,
Washington, D.C.

DEAR MR. SPEISER: Commissioner Thrower has asked me to respond to your October 22 letter regarding our Manual Supplement "Protection of the President: Guidelines for Reporting Information." If you have a copy of the document in question, you will see that the guidelines in question were issued by the United States Secret Service. The guidelines were distributed to Internal Revenue Service employees in an effort to be of maximum assistance to Secret Service in meeting their protective responsibilities.

I have referred your letter to the Secret Service, and I assume you will be hearing from that office in the near future.

Sincerely,

LEON C. GREEN,
Deputy Assistant Commissioner.

[From manual Supplement, U.S. Treasury Department, Internal Revenue Service, Aug. 22, 1969]

PROTECTION OF THE PRESIDENT: GUIDELINES FOR REPORTING INFORMATION

SECTION 1. BACKGROUND

The U.S. Secret Service is charged with the responsibility of protecting the President and certain other high-level Government officials and public figures. This responsibility includes the evaluation of all information concerning threats against the personal safety of those being protected. It is incumbent upon the Internal Revenue Service, along with other agencies, to assist the Secret Service in this responsibility by the timely reporting of any information which will help that organization to do its job effectively.

SECTION 2. PURPOSE

This Manual Supplement provides: *U.S. Secret Service Liaison Guidelines*, which outlines the type of information most useful to the Secret Service (see

Attachment 1); instructions for reporting this information; and a list of Secret Service field offices.

SECTION 3. GUIDELINES

Employees should: familiarize themselves with the attached document, *U.S. Secret Service Liaison Guidelines;* be alert to circumstances which warrant their consideration; report information in accordance with Section 4 of this Manual Supplement; and upon request, cooperate fully with the Secret Service in discharging their responsibilities in this area.

SECTION 4. REPORTING PROCEDURES

.01 As indicated in the Secret Service guidelines, information should be promptly referred to the Secret Service Washington Office. Employees will use their discretion to determine the most judicious method of notifying the Secret Service. If the referral is urgent, employees are authorized to telephone the nearest Secret Service Office. When time permits, a written report should be sent to the Secret Service Washington Office. Attachment 2 to the Manual Supplement contains a list of Secret Service field offices giving their addresses and telephone numbers.

.02 In all cases, the person making the referral will prepare a written report for his own file. This report will contain: all the information given to the Secret Service, the Secret Service office and personnel notified, and the time and date of the referral.

SECTION 5. EFFECT ON OTHER DOCUMENTS

IRM 1941.7 is supplemented; and Manual Supplement 19G–46, dated June 1, 1966, is superseded.

(Attachment)

U.S. SECRET SERVICE LIAISON GUIDELINES

Subject to the direction of the Secretary of the Treasury, the United States Secret Service is charged by Title 18, U.S. Code, Section 3056, with the responsibility of protecting the person of the President of the United States, the members of his immediate family, the President-Elect and Vice President, or other officer next in the order of succession to the Office of President, and the Vice President-Elect, protect the person of a former President and his wife during his lifetime, the person of the widow of a former President until her death or re-marriage, and minor children of a former President until they reach 16 years of age, unless such protection is declined, protect persons who are determined from time to time by the Secretary of the Treasury, after consultation with the Advisory Committee as being major Presidential and Vice Presidential candidates which should receive such protection (unless the candidate has declined such protection).

Detecting and arresting any person committing any offense against the laws of the United States relating to coins, obligations, and securities of the United States and foreign Governments. Several other responsibilities are delegated to the U.S. Secret Service by the Secretary of the Treasury, such as investigation of violations of the Gold Reserve Act, and such other functions as are authorized by law.

Effective liaison with other law enforcement and Government agencies is necessary to insure we receive all information they may develop regarding any of our responsibilities. A Special Agent of the Liaison Division, U.S. Secret Service, will maintain contact with your agency at a headquarters level. Certain guidelines are set forth below which may assist you in determining our interests.

1. PROTECTIVE INFORMATION

A. Information pertaining to a threat, plan or attempt by an individual, a group, or an organization to physically harm or embarrass the persons protected by the U.S. Secret Service, or any other high U.S. Government official at home or abroad.

B. Information pertaining to individuals, groups, or organizations who have plotted, attempted, or carried out assassinations of senior officials of domestic or foreign Governments.

C. Information concerning the use of bodily harm or assassination as a political weapon. This should include training and techniques used to carry out the act.

D. Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.

E. Information on any person who makes oral or written statements about high Government officials in the following categories: (1) threatening statements, (2) irrational statements, and (3) abusive statements.

F. Information on professional gate crashers.

G. Information pertaining to "Terrorist" bombings.

H. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war.

I. Information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas.

J. Information regarding civil disturbances.

2. COUNTERFEITING AND FORGERY INFORMATION

A. Information regarding counterfeiting of U.S. or foreign obligations, i.e., currency, coins, stamps, bonds, U.S. Treasurer's checks, Treasury securities, Department of Agriculture food stamp coupons, etc.

B. Information relating to the forgery, alteration and fraudulent negotiation of U.S. Treasurer's checks and U.S. Government bonds.

3. GOLD AND "GOLD COIN" INFORMATION

A. Gold regulations prohibiting the acquisition, holding, transportation, importing, and exporting of gold by persons subject to the jurisdiction of the United States. Gold in its natural state may be purchased, held, sold or transported within the United States and may also be imported without a license.

B. Gold coins of recognized special value to collectors may be acquired, held and transported within the United States and may be imported as permitted by the gold regulations.

Routine reports may be mailed to the U.S. Secret Service, Liaison Division, Room 825, 1800 G Street, N.W., Washington, D.C. 20226, or handled during personal liaison contact.

Emergency information, especially in reference to Presidential protection, should be reported immediately by telephone to the nearest U.S. Secret Service field office or the U.S. Secret Service Intelligence Division, Washington, D.C. Area Code 202–WO4–2481; (government Code 184–2481).

[70 Duke Law Journal (1970)]

COMPUTERS AND PRIVACY: A PROPOSAL FOR SELF-REGULATION*

(By Edward J. Grenier, Jr.*)

In framing the issues of its landmark Computer Inquiry, the Federal Communications Commission cited the critical importance of the preservation of information privacy:

"Privacy, particularly in the area of communications, is a well established policy and objective of the Communications Act. Thus, any threatened or potential invasion of privacy is cause for concern by the Commission and the industry. In the past, the invasion of information privacy was rendered difficult by the scattered and random nature of individual data. Now the fragmentary nature of information is becoming a relic of the past. Data centers and common memory drums housing competitive sales, inventory and credit information and untold amounts of personal information, are becoming common. This personal and proprietary information must remain free from unauthorized invasion or disclosure, whether at the computer, the terminal station, or the interconnecting communication link." [1]

Congress, too, has demonstrated an increasing concern with the possible threats to individual privacy which might result from the establishment, by the federal government or by private industry, of a national data bank.[2] In fact Paul Baran of Rand Corporation, testifying several years ago before a congressional

Footnotes at end of Article.

subcommittee, stated that the United States is unconsciously moving toward an integrated, nationwide, automated information system:

"My thesis is this: Today we are already building the bits and pieces of separate automated information systems in both the private and government sectors that so closely follow the pattern to the present integrated communications structure that a de facto version of the system you are now pondering is already into the construction phase. It is in many ways more dangerous than the single data bank now being considered." [3]

Although the threat posed by automated information systems to the privacy of *individuals* is perhaps the most dramatic aspect of the "computer revolution," another very important aspect is the possibility of unauthorized disclosure of *proprietary data*. The "privacy problem" in both of these contexts is most acute where the separate proprietary data of a large number of businesses or sensitive personal information about thousands of individuals is stored or processed in multiprogrammed, time-sharing data processing systems and transmitted to and from the processing and storage units over common communications lines. In such systems there exists at numerous points a high potential for "information leakage," including leakage due to hardware and software failures and wire taps.[4]

In addition to examining both of these aspects of the privacy problem from the point of view of the computer system operator, this article proposes the establishment of a logical legal framework which would serve the public interest by assuring, first, that computer systems which handle sensitive individual or proprietary data will meet certain minimum standards established for the protection of privacy, and, second, that computer system operators will be able to continue to operate in a competitive economy unhindered by either overly restrictive governmental regulation or the fear of private legal liability. The analysis and suggestions herein set forth are relevant to all types of computer systems which store information or use computer programs belonging to persons or entities other than the computer system operator or which collect and store information about private individuals.[5]

The computer industry, which when viewed in its broadest significance extends from manufacturers of main frame hardware to computer service bureaus and computerized information services, should now cooperate with the communications industry to adopt and implement, under the auspices of the federal government, a comprehensive system of self-regulation to ensure the privacy and security of data. As a corollary of such a scheme, computer systems complying with the established standards [6] should be freed from certain types of civil legal liability for the unauthorized or accidental divulgence of individual or proprietary information.[7]

THE PRESENT LEGAL SITUATION: A STUDY IN UNCERTAINTY

For the purpose of analyzing the present legal controls pertinent to privacy and the computer, it will be helpful to consider a few illustrative situations:

"1. Computer service company A operates a multi-programmed, time-sharing, remote-access data processing system. It services 25 customers scattered over a wide area, each with at least one remote terminal device. Each of A's customers stores at least one proprietary program and a good deal of data in A's system. Companies X and Y are competitors and are both customers of A. Let us suppose that company X has been able to obtain confidential data belonging to Y at X's remote terminal.

"2. Assume the same basic set of facts with the exception that A has 500 customers, most of which are very small.

"3. Company A runs a computerized information service containing personal data about thousands of individuals, including credit data, medical data, employment data, and educational data. A offers this service to carefully selected classes of subscribers, each of whom promises to use the information for only circumscribed and legitimate purposes.[8] Company A's subscribers are linked to its computer system by remote terminal. Mr. X, a nonsubscriber, manages to tap into company A's system and connect an unauthorized remote terminal, thereby gathering information about a number of individuals. The information so obtained is used in an article which he publishes in a national magazine.

"4. Assume the same facts as in example 3, except that a programmer-employee of company A, without authority, extracts information about some individual from the system and sells such information to Mr. X."

Footnotes at end of Article.

Although the number of possible variations is almost without limit, these four examples are sufficient to illustrate some of the difficulties which computer service companies may face.

From the point of view of the computer service company, the first two examples present issues of contractual or, possibly, tort liability.[9] The customer whose *proprietary* data has been obtained without authority by some third party might well have a claim for breach of contract against the computer service company. However, the results in such a situation can be quite diverse. If the computer service company is dealing with large, sophisticated customers, service contacts are likely to be thorough and well-defined, specifying with detail the degree of privacy and security of data promised by the company and expected by its customer. On the other hand, if the computer service company's customers are small and perhaps less sophisticated, the contract between them may tend to be of the boiler plate variety and may not contain provisions adequate to protect the privacy and security of data. But uncertainty, rather than a complete absence of protection, is more likely to be the case.[10] Unfortunately, the outcome in any specific situation will depend upon the prevailing business practices and governing standards in the state involved.

Examples 3 and 4 squarely raise the issue of the extent to which an *individual's* "right of privacy" will be afforded legal protection.[11] Although most privacy cases involving the disclosure of *individual* information are likely to arise as tort actions, situations could arise in which an individual might have a claim based upon the law of contract. For example, assume that a computer service company enters into a contract with company X to store personal data concerning some one thousand employees of X and to furnish the data to X upon request. Assume further that the contract includes specific provisions for protecting the privacy of the individuals involved. If the computer company breaches the contract by allowing information to fall into the hands of a third person who uses it to the injury of the employees, the injured employee might seek recovery against the computer service company as a third party beneficiary of the computer service contract.[12]

In most situations, however, an individual's claim that his privacy had been violated would have to be founded upon the tort of invasion of or interference with privacy. Although of relatively recent judicial recognition,[13] this tort has developed to the point where one noted commentator has been able to discern the existence of four separate torts under the rubric "invasion of privacy";[14] (1) unreasonable intrusion upon the seclusion of another or into his private affairs;[15] (2) appropriation of an individual's name or likeness;[16] (3) unreasonable publicity given to another's private life, or public disclosure of a private fact about an individual;[17] and (4) publicity which places another in a false light in the public eye.[18]

The tort doctrine regarding the protection of privacy, in its present state of development, quite possibly would not provide a basis for a finding of liability against the computer service company in either example 3 or 4, where we have assumed that the computer company took no deliberate action to injure the plaintiff. However, the law of privacy has developed in response to the changing conditions of society, and the advent of the computer age is almost certain to result in a further judicial expansion of the doctrine—perhaps with legislative help.[19] Although four states apparently still reject the right of privacy in its entirety,[20] judicial expansion of the doctrine continues. In *Griswold v. Connecticut*,[21] for example, the Supreme Court seemed to find, in a context quite far removed from the fourth amendment prohibition against unreasonable searches and seizures, a constitutionally protected right of privacy inherent in several amendments.[22]

Of special significance is the recent New York decision in *Nader v. General Motors Corp.*,[23] which extended the *Griswold* rationale prohibiting the violation of a constitutional right to privacy to invasions by private corporations, not the state. The court implicitly found that state inaction—the refusal by the state court to entertain a lawsuit alleging a violation by the corporation of the plaintiff's constitutional right to privacy—constituted sufficient "state action" to invoke the protection of the fourteenth amendment.[24] If the holding in *Nader* survives, the implications for the computer industry could be far-reaching.[25]

There can be no doubt that the computer service industry, dealing as it does with personal data on hundreds or thousands of individuals, strongly affects the public interest.[26] Indeed, against the background of expanding computer services the need for a further extension of the doctrine of right of privacy has been

Footnotes at end of Article.

vigorously asserted.[27] Thus, one commentator has recently noted that "[t]he concept of privacy held by most courts, considered revolutionary during the Warren-Brandeis era, seems more fitted for the 19th century rather than the 20th; a 'new privacy' must be formulated to protect the individual from the technological advances of the computer age." [28] Another commentator recently advanced the thesis that the fifth amendment prohibition against the taking of private property by the government without just compensation, applicable to the states through the fourteenth amendment, should be extended to a similar destruction or diminution of the right of individual privacy.[29] Furthermore, actions by large public corporations which result in a diminution of an individual's privacy should be regarded as equivalent to state action and therefore subject to the payment of "just compensation." [30] The growing tendency to extend the bounds of privacy protection is thus manifest.[31] If, because of their vast informational storage and ready access capabilities, computers and computer systems become generally regarded as great potential threats to the individual's right of privacy, it would not be surprising to find courts holding computer service companies liable for the unauthorized disclosure of information about an individual.[32] Moreover, the court might go beyond the traditional concept that the defendant must be guilty of an intentional or deliberate wrongdoing in order to be held liable under an invasion of privacy theory and hold computer companies liable for negligently permitting an unauthorized release of information. Indeed, if the information is sensitive enough and the damage from release is devastating enough, a court might be tempted to dispense even with the requirement of negligence and simply hold the computer company *absolutely* liable for the unauthorized release.[33] Whether the computer company's failure is technological [34] or human [35] should make no difference.

The law usually has evolved to keep pace with changing social, political, moral, and economic circumstances. For those who might dismiss as "mere speculations" the above thoughts about the possible evolution of the law of privacy in response to the computer revolution, it would be instructive to consider a statement by Professor Arthur Miller during a recent symposium on the computer and privacy:

"The computer is a many-splended animal. It is myopic to think of it as little more than a high speed calculator with a gland condition. It's much more than that. Modern information transfer technology in time will prove to be the heart of a new communications network, a communications network that differs from many of the communication networks that we are familiar with, such as telephones, telegraph, radio, television and newspapers, only in technological and media terms. Accordingly, the computer must be dealt with as a communications network.

"In short, I am suggesting that we are dealing with a problem of immense importance. . . . [G]iven the large stakes, we should not think simply in terms of the ethical or moral implications of a National Data Center, or any other type of a data center. We must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of existing systems or assumptions about the immutability of the technology.[36]

It is apparent that the legal protection given to the right of privacy is far from static and may, within the reasonably foreseeable future, undergo marked changes. However, except insofar as the changes may be founded upon federal constitutional doctrines, the developing principles may vary markedly from state to state because the basic law involved will be state, not federal, law.[37] For the computer service company, this could mean facing different standards of liability in fifty different jurisdictions for the unauthorized disclosure of information—an unhappy prospect for companies who do a national or regional business.

At present, there is no body of federal law governing privacy which might "preempt" state law as applied to computer systems. After receiving the many detailed and thoughtful comments in its Computer Inquiry and the analysis of the responses prepared by the Stanford Research Institute, as well as the Institute's own recommendations, the FCC has decided that it must await the collection of additional information before deciding whether to exercise its regulatory authority in the area of privacy and security of data during transmission and storage.[38]

Although it did take a significant step in the privacy area in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[39] Congress has not acted decisively in this area. In Title III, Congress (1) outlawed the interception and disclosure of wire or oral communications, except as specifically authorized in

Footnotes at end of Article.

the statute pursuant to court order;[40] (2) amended section 605 of the Communications Act of 1934[41] to take into account the foregoing addition to the federal criminal code;[42] and (3) established a "National Commission for the Review of Federal and State Laws Relating to Wire Tapping and Electronic Surveillance," which is to study the entire wiretapping and electronic surveillance situation and make a final report within seven years.[43] One interesting feature of this act is that it gives a civil cause of action for damages to "any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter. . . ."[44] Although this provision for civil damages in Title III will provide a new, and perhaps potent, remedy to the individual citizen in protecting his privacy, the remedy reaches only one aspect of the privacy problem in data processing, and it certainly does not in any way preempt the various provisions of state law dealing with invasions of privacy. First, the remedy is limited only to persons whose wire or oral *communications*[45] are intercepted, disclosed, or otherwise used in violation of the act. Thus, this remedy on its face does not reach the problem of the unauthorized disclosure of stored information about an individual, which is *not* "communicated" by the individual *himself* to someone else.[46] Secondly, it is not entirely clear whether the act's sanctions will even reach the problem of interception of data being transmitted to or from a data bank, or the disclosure of such data after interception. The term "intercept," as used in the act, means the "*aural* acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical or other device."[47] Query whether transmitted data is subject to such "aural acquisition," at least in the case of data sent over a special digital communications network using time division multiplexing techniques; query whether courts would reach different conclusions depending upon the technical nature of the communications network over which the data traveled.[48]

A RATIONAL SOLUTION: SELF-REGULATION BY THE COMPUTER INDUSTRY UNDER GOVERNMENTAL AUSPICES

It is estimated that by the late 1970s, the traffic volume over the nation's telephone network will be about equally divided between voice and data transmission,[49] representing a far greater use of the telephone network for data transmission than at present. By 1975 more than 60 percent of the computer hardware used in the United States will be tied into the public communications system, and estimates for 1984 have run as high as 90 percent.[50] Thus, we are on the verge of an explosion in remote access data processing, including a great number of time-sharing, real-time systems. The trends in the law discussed above[51] may well be accelerated by the quickening pace of technological progress.

The choice lies with the computer industry. It can go along and let events unfold in an unstructured, haphazard manner and thereby permit others to fashion for it the basic standards and rules governing the conduct of its business, or it can itself initiate rational means to control its own destiny and at the same time serve the public interest by assuring privacy and security of data, in both transmission and storage. In an industry whose whole thrust is to bring rational order out of the potential chaos unleased by the information explosion, the choice seems clear. Working from the foundations already laid, the computer industry should pull together, develop, and then enforce standards of construction and operation for computer systems which process data of such a nature that privacy or security are necessitated.

Before detailing the mechanics of this proposal it would be well to point out what is not being proposed. The regulation contemplated would not deal with such matters as the rates or prices to be charged by computer service companies, the rate of return they should earn, the terms and conditions of their sales to their customers, or other matters relating to traditional economic or rate regulation.[53] Rather, the industry, under federal governmental auspices, would develop standards to assure that computer systems will incorporate a reasonable degree of privacy protection and will be operated to achieve the desired degree of privacy and security of data necessary in any given circumstances.[53]

Any program of self-regulation should include at least the following features:

1. The program should be specifically authorized and established by federal statute, a prerequisite which would avoid the antitrust problems that inevitably arise where competitors or potential competitors associate to formulate industry standards.[54] Indeed, the statute should grant a specific antitrust exemption for activities within its scope.

Footnotes at end of Article.

2. Because the program is one of *self*-regulation, some statutory mechanism should be established to permit governmental administrative review of regulatory standards, upon the complaint of interested persons, before they become effective. Such a mechanism would provide customers and potential customers of the computer service industry, as well as private individuals, with an opportunity to express their views on proposed standards.[55]

3. An organization composed of representatives of the computer industry should be established to promulgate and enforce the desired standards. Such an agency should be specifically recognized and granted authoritative powers by federal statute, and its decisions in promulgating standards and in supervising the operations of the computer service industry should be final, though subject to specific types of review by an appropriate government administrative agency [56] and, ultimately, limited judicial review.[57]

4. The industry agency charged with promulgation and enforcement should have the power of periodic inspection to assure compliance with standards regarding the privacy and security of data.

5. The agency should have specific power at least to conciliate disputes between customers and computer service companies and between individual citizens and computer service companies, arising from, or related to, the standards formulated by the industry agency.[58] Perhaps such conciliation can be made a condition precedent to the bringiing of any lawsuit involving the standards or application of the standards.[59]

6. The industry agency should, under guidelines set forth in the federal statutes establish a licensing or certification system for computer systems which will handle information about individual citizens or proprietary data belonging to persons or companies other than the computer system operator. Before any such computer system is permitted to commence operation, it should be required to obtain a license certifying that the industry standards for the protection of privacy and security of data have been met. Such standards should cover not only the technical aspects of the computer system, but also the qualifications of key personnel having access to the system. In connection with the licensing procedure, the applicant should be required to show that it has developed, and will use, appropriate procedures to comply with the standards and to assure that its key employees comply with the industry's code of conduct. As noted above, after initial licensing the industry's agency should have continued inspection powers to assure that the licensee complies with industry standards. Again, both in connection with initial licensing and any subsequent industry proceeding brought to enforce compliance with standards, there should be review by the concerned governmental agency and, ultimately, limited judicial review. In the event of proposed major alterations in the system, a system licenses should be required to go through a new licensing procedure.

7. The industry agency should have power to promulgate and enforce a code of conduct for programmers and other key personnel working with computer system to which industry standards apply. Sanctions would be imposed upon individuals violating the code of conduct, subject, of course, to administrative review by a government agency and, ultimately, limited judicial review. Such sanctions might include the imposition of fines, with the maximum fixed by statute, suspension from employment, and, in the case of the most flagrant violations, even complete expulsion from the computer service industry.[60]

8. The federal authorizing statute should specifically provide that industry standards will be recognized and given full force and effect in all judicial proceedings, both state and federal. In fact, the statute should provide that, in the absence of an express agreement to the contrary between a computer service company and its customer, the company will not be liable for any loss or destruction of data, or "leakage" of data to unauthorized persons, if the company's computer system has been duly licensed and certified to be in compliance with the industry association's standards, and if in fact the system was in compliance with such standards at the time of the loss, destruction, or unauthorized disclosure. This same exemption from liability should apply, in the case of a claim against the computer service company by an individual on account of unauthorized disclosure of data about such individuals.[61]

The preceding framework is necessarily a very broad-brush treatment of a highly complex subject. However, if the idea of self-regulation is accepted and adopted by the computer industry, the foregoing guidelines can be a point of departure in constructing the system. What is needed is a broad consensus within

Footnotes at end of Article.

the industry as to the route to be followed, which can then be translated into concrete legislation and a detailed plan of operation.

On the technical side, considerable effort over the past few years has been devoted to developing and improving hardware and software techniques for assuring privacy and security of data during both transmission and storage.[62] In addition, many of the comments filed in the FCC's Computer Inquiry described various techniques used to assure privacy in remote access data processing applications.[63] Thus there is a readily available body of recorded experience and thoughtful comment upon which the standards makers could draw in beginning their complex task.

One aspect of the foregoing proposal for self-regulation must be given special attention. In the case of remote access data processing the communications links between the remote terminals and the computers must be considered a part of the computer "system" to be licensed or certified if there is to be really effective privacy protection. Yet, in virtually all instances, the communications links will be furnished by common carriers *not related* to the computer service company seeking the license or certification.[64] Thus neither the computer company nor the industry agency proposed above will have control over the degree of privacy protection afforded by a very important link in the computer "system" to be licensed or certified.

The solution to this problem does not rest in making the communications common carriers subject to regulation by the industry agency proposed in this article. Any regulatory scheme which subjects a company to regulation directly by its customers must be viewed with at least a healthy skepticism. Thus the communications common carriers should not be subject to regulation by the computer industry agency insofar as these carriers provide communications services in connection with remote access data processing.[65] Moreover, any such attempted regulation of the communications activities of the communications common carriers by the computer industry agency might well conflict with existing regulation by the FCC on the national level and by public service commissions on the state level.

Rather, the solution to the problem would appear to lie in a well-organized system of cooperation between the communications carriers and the computer industry agency, with regulatory assistance from the FCC as required. There should be a continuing formalized liaison between the communications carriers and the computer industry agency, perhaps in the form of one or more representatives of the communications industry working full time in the liaison activity. Such liaison could function effectively in at least two types of situations: (1) when the industry association is formulating privacy protection standards, it should consult closely with the communications industry to assure that tariffed offerings affording the desired degrees of privacy protection in various situations will be available to the computer service industry; (2) if communications problems arise in connection with any particular licensing proceeding under the above proposal, the suggested liaison could help to resolve the problem, possibly through inducing the carrier involved to make a new tariff offering or to amend an existing tariff offering.

Of course, if the liaison activity should fail to resolve any really significant problem, recourse could be had to the FCC or the appropriate state public service commission. To ensure that the FCC will be able to act effectively and expeditiously, the federal statute authorizing the system of industry self-regulation should expressly give the FCC whatever additional power that may be necessary.[66]

There is presently one highly successful example of industry self-regulation under federal governmental supervision. For some thirty years, the National Association of Security Dealers [NASD] has created and enforced a thorough program of self-regulation for the securities industry, including member broker-dealer firms and individual registered representatives. Its principal activities include the administration of examinations to assure the qualifications of employees in the securities industry, the promulgation and enforcement of rules of conduct and fair practice for the securities industry, and the adjustment of grievances between members and between members and the public.[67] One of the most effective tools in NASD's program of self-regulation is its power to examine the books and records of member firms to ensure compliance with NASD rules as well certain federal regulations. This is equivalent to the inspection program proposed above for the computer industry. In addition, NASD operates a program of voluntary arbitration, both for disputes among its members and for disputes between the public and its members. In the case of disputes of the latter variety, the arbitration panel consists of three members of the public and two representa-

Footnotes at end of Article.

tives from the securities business. In a member versus member contest, the panel consists of from three to five representatives from securities industry.

Although there are obvious differences between the securities industry and its problems and the computer industry and its problems, NASD constitutes a valid precedent for the type of self-regulatory industry agency proposed herein. By adopting a NASD-type approach, the computer industry can assure the creation of a rational and orderly legal framework for resolving the increasing pressing problem of privacy in the context of the computer revolution and, at the same time, assure that regulation will be in the hands of persons thoroughly cognizant of the complexities of the situation and the need for protection of individual rights and proprietary interests in data and programs—all to the benefit of the public interest.

FOOTNOTES

*Member, District of Columbia Bar, B.A. 1954, Manhattan College; L.L.B. 1959, Harvard Law School.

[1] FCC Notice of Inquiry, Docket, No. 16979, 7 F.C.C. 2d 11, 16–17, 8 P & F Radio Reg. 2d 1567, 1572 (Nov. 9, 1966) [hereinafter cited as *Computer Inquiry*].

[2] *See generally Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess. (1966) [hereinafter cited as *Gallagher Hearings*]; Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 Harv. L. Rev. 400 (1968); *Research Project—Computerization of Government Files, What Impact on the Individual?*, 15 U.C.L.A.L. Rev. 1371 (1968).

[3] *Gallagher Hearings* 122.

[4] *See* Ware, *Security and Privacy in Computer Systems*, Proceedings, 1967 Spring Joint Computer Conference 279, 280 figure 1. Effective protection of both individual privacy and proprietary data also demands control over the amount and character of the data input entering the system. *See* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 Mich. L. Rev. 1091, 1214–71, 1229–30 (1969) [hereinafter cited as Miller]. Regulation of data input is beyond the scope of this article which is directed solely to controls in the storage and utilization of the data previously collected.

[5] An obvious example of the latter is the automated credit bureau. Credit Data Corporation maintains a large scale, on-line computerized credit information system with data centers located in Los Angeles and New York City. Response of Credit Data Corp. to FCC Computer Inquiry, March 5, 1968. *See generally* Miller 1140–54.

[6] See notes 54–61 *infra* and accompanying text.

[7] This paper does not deal with the problems presented by the *voluntary* disclosure by the system operators of private information about individuals stored in computer systems or questions relating to the accuracy of information about individuals contained in such systems. For discussions of some of the problems involved in the storage of inaccurate information about individuals and the voluntary disclosure of information about individuals, whether accurate or inaccurate, by the custodians of such information, see Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personnel Data*, 31 Law & Contemp. Prob. 342 (1966); Sills, *Automated Data Processing and the Issue of Privacy*, 1 Seton Hall L. Rev. 7 (1970); Note *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 Geo. L.J. 509 (1969).

[8] What constitutes "legitimate" voluntary disclosure of information by the information service company is beyond the scope of this paper. See not 7 *supra*.

[9] *See generally* Miller 1156–73.

[10] *See* Lickson, *Protection of the Privacy of Data Communications by Contract: Another Case Study on the Impact of Computer Technology on the Law*, Bus. Law, July 1968, at 979–80.

[11] Under certain variations of these examples, the contractual rights of the computer service company's customer may also be involved.

[12] *See generally* Restatement of Contracts §§ 133–47 (1932).

[13] The Supreme Court of Georgia is considered to have laid the foundation for recognition of a right to privacy as a fundamental, legally protectible interest in Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68, 69–70 (1905). Of course, the intellectual foundation for recognition of invasion of privacy as a separate tort had been laid in Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[14] Prosser, *Privacy*, 48 Calif. L. Law. 383, 389 (1960).

[15] *See e.g.*, Le Crone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E. 2d 533 (1963) (wiretapping of an individual's telephone).

[16] *See, e.g.*, Flake v. Greensboro News Co., 212 N.C. 780, 195 S.E. 55 (1938) (photograph of an actress used in a bread advertisement).

[17] *See, e.g.*, Brents v. Morgan, 221 Ky. 765, 299 S.W. 967 (1927) (sign in garage window stating that the plaintiff's account with the garage has been unpaid for a long time).

[18] *See, e.g.*, Peay v. Curtis Publishing Co., 78 F. Supp. 305 (D.D.C. 1948) (newspaepr article on the alleged practices of Washington cab drivers in cheating the public on fares, making use of the plaintiff's photograph to illustrate the article).

[19] For example, Congress is now considering legislation which would regulate the activities of credit bureaus and credit investigating agencies, a field in which the computer has been playing an ever-increasing role. S. 823, 91st Cong., 1st Sess. (1969); H.R. 7874, 91st Cong., 1st Sess. (1969); H.R. 9150, 91st Cong., 1st Sess. (1969); H.R. 9888, 91st Cong., 1st Sess. (1969). The Senate passed S. 823 on Nov. 6, 1969, 115 Cong. Rec. 13,905–11 (daily ed. Nov. 6, 1969) and reported it to the House Committee on Banking and Currency on Nov. 12, 1969. Hearings have been held this spring before the House Committee.

[20] These states are Nebraska, Rhode Island, Texas, and Wisconsin. Restatement (Second) of Torts, ch. 28A, at 100 (Tent. Draft No. 13, 1967).

[21] 381 U.S. 479 (1965).

[22] *See also* Tehan v. Shott, 382 U.S. 406 (1966), where the Court pointed out that the fifth amendment guarantee against self-incrimination is really in part an extension of an individual's right to privacy and "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" *Id.* at 414 n. 12.

[23] 57 Misc. 2d 301, 292 N.Y.S. 2d 514 (Sup. Ct. 1968), *aff'd* 298 N.Y.S. 2d 137 (App. Div. 1969).

[24] *Id.* at 305, 292 N.Y.S. 2d at 518.

[25] The Appellate Division, in affirming the trial court's refusal to discuss the case, held that it need not pass upon the constitutional grounds advanced by the trial court, 298 N.Y.S. 2d at 141. We shall have to await further litigation to test the implications of *Nader*.

[26] *See generally* A. Westin, Privacy and Freedom (1967); *Gallagher Hearings, supra* note 2; Pipe, *Privacy: Establishing Restrictions on Government Inquiry*, 18 Am. U.L. Rev. 516 (1969); Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 Geo. L.J. 509 (1969); *Research Project—Computerization of Government Files, What Impact on the Individual?* 15 U.C.L.A.L. Rev. 1371, 1375 (1968) (foreward by Mr. Justice Douglas).

[27] Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 Geo. L.J. 509 (1969).

[28] *Id.* at 532.

[29] Comment, *Privacy, Property, Public Use, and Just Compensation*, 41 S. Cal. L. Rev. 902, 909 (1968).

[30] *Id.* at 913. The author's main point is made in the following statements:

"It can be argued that all large public corporations, such as Time, Inc., whose activity has as great a societal impact as does most governmental action, should be subject to the same constitutional limitations as is the government. Their activity should be labelled 'public,' rather than 'private,' in contradistinction to an individual's activity. . . . In short, most corporations are, at least in part, fulfilling interests of the state, and no longer fulfilling the traditional justifications of private property. In these instances they ought to be subject to the same constitutional limitations as are imposed that private property cannot be taken for a public use without payment of just compensation." *Id.* at 913–14.

And, as noted, the author would equate the "right of privacy" to "private property" and would require the payment of just compensation for any action which results in a destruction or diminution of an individual's right of privacy.

[31] The American Law Institute, in a tentative draft of a portion of a new Restatement of Torts, commented that new forms of the tort of invasion of privacy in addition to the four basic types already generally recognized by the courts may emerge, especially in light of recent decisions by the United States Supreme Court. Restatement (Second) of Torts § 652A, comment c (Tent. Draft No. 13, 1967). *See also* Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's, Pt. II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66 Colum. L. Rev. 1205, 1232 (1966).

[32] This might prove true whether the companies are service bureaus, information services, or some other type of computer service company.

[33] Early manifestations of the theory of strict liability are shown in Huthringer v. Moore, 31 Cal. 2d 489, 19 P.2d 1 (1948); Ball v. Nye, 99 Mass. 582 (1863) (percolation of filthy water); Cahill v. Eastman, 18 Minn. 324 (1872) (underground water tunnel). For an example of statutory extension of this principle, see the relevant portions of the Federal Safety Appliance Act, 45 U.S.C. §§ 1–60 (1964).

[34] See, for example, situations 1, 2, and 3, text at 497.

[35] See, for example, situation 4, text at 497–98.

[36] *Symposium: Computers, Data Banks, and Individual Privacy*, 53 Minn. L. Rev. 211, 225–27 (1967). The growing concern over protecting privacy in our era of technological explosion is evidenced by the fact that most of the May-June 1969 issue of Think, the very informative magazine published by IBM, is devoted to a special report on privacy. The articles include Miller, *Psychological Testing: Can We Minimize the Perils?*, Think, May-June 1969, at 24; Ruggles, *How a Data Bank Might Operate*, *id.* at 22; Westin, *Life, Liberty, and the Pursuit of Privacy*, *id.* at 12; Westin, *New Lines Will Protect Your Privacy*, *id.* at 27. Professor Westin's concluding remarks in his first article are especially illuminating: "American Society now seems ready to face the impact of science on privacy. Failure to do so would be to leave the foundations of our free society in peril." Westin, *Life, Liberty, and the Pursuit of Privacy*, *id.* at 21. In his second article, Professor Westin points out that many organizers of private data banks, in growing recognition of the privacy problem presented by the computer revolution, are establishing administrative controls to assure the protection of privacy. Westin, *New Laws Will Protect Your Privacy*, *id.* at 31.

[37] *See* Erie R.R. v. Tompkins, 304 U.S. 64 (1938), which laid to rest the notion that there is any generally applicable federal common law to be applied by the federal courts in considering "general" issues in diversity cases. For a more thorough discussion of the *Erie* line of cases, see 1 A. J. Moore, Federal Practice ¶ 0.318 (2d ed. 1965); Friendly, *In Praise of Erie—And of the New Federal Common Law*, 39 N.Y.U.L. Rev. 383 (1964).

[38] *Computer Inquiry*, Report and Further Notice of Inquiry, 17 F.C.C. 2d 587, 592, 16 P & F Radio Reg. 2d 1505, 1510 (1969); *Computer Inquiry*, Notice of Proposed Rule Making and Tentative Decision, 18 P & F Radio Reg. 2d 1713, 1718 (1970). The regulatory authority of the FCC in this area may, of course, be limited in the absence of additional legislation.

[39] 18 U.S.C. §§ 2510–20 (Supp. IV, 1969).

[40] *Id.* §§ 2511, 2515–19.

[41] 47 U.S.C. § 605 (Supp. IV, 1969).

[42] § 803, 82 Stat. 212, 223 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

[43] § 804, Stat. 212, 223–25 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

[44] 18 U.S.C. § 2520 (Supp. IV, 1969).

[45] As used in the statute, "wire communication" means:

any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications. *Id.* § 2510(1).

An "oral communication" means: "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation. *Id.* § 2510(2).

[46] *See* Miller 1201.

[47] 18 U.S.C. § 2510(4) (Supp. IV, 1969) (emphasis added). It remains to be seen how the definition will be interpreted. The legislative history of the Act shows clearly that Congress was preoccupied with the interception of voice communications, whether by wiretapping or other electronic devices. *See* S. Rep. No. 1097, 90th Cong., 2d Sess. 217–218 (1968). The few cases that have cited Title III of the Act have all been criminal cases or civil antitrust cases closely related to criminal cases and have all dealt with voice communications. *See, e.g.*, Alderman v. United States, 394 U.S. 165, 175 & nn. 8–9 (1969); United States v. McCarthy, 292 F. Supp. 937, 943 (S.D.N.Y. 1968); Philadelphia Housing Authority v. American Radiator & Standard Sanitary Corp., 291 F. Supp. 247, 249–50 (E.D. Pa. 1968); United States v. Schipani, 289 F. Supp. 43, 60 (E.D.N.Y. 1968); United States v. American Radiator & Standard Sanitary Corp., 288 F. Supp. 701, 706–07 (W.D. Pa. 1968).

[48] For example, the courts might arguably distinguish between interception of data transmitted by the regular analog telephone network and that carried over a special digital network. *See generally* Miller 1206.

[49] *See* Chaney, *Data Transmission Basics*, Communications, Mar. 1969, at 27; *cf.* Irwin, *Computers and Communications: The Economics of Interdependence*, 34 Law & Contemp. Prob. 360, 361 (1969).

[50] Note, *Computer Services and the Federal Regulation of Communications*, 116 U. Pa. L. Rev. 328 (1967).

[51] See notes 13–17 *supra* and accompanying text.

[52] The respondents to the FCCs Computer Inquiry, including the Department of Justice, generally agreed that the computer service industry should be permitted to develop in the free competitive economy, and not as a regulated utility. *See* L. Krause, *Analysis of Policy Issues in the Responses to the FCC Computer Inquiry*, Standard Research Institute Report No. 7379B–2, at 22–26 (1969). The author agrees. For a thorough discussion of the issues involved, see S. Mathison & P. Walker, Computers and Telecommunications: Issues in Public Policy 16–19 (1970). The FCC as of this time, agrees. *See Computer Inquiry*, Tentative Decision, 1718–22.

[53] These standards should be defined to the greatest extent possible.

[54] For a discussion of the limitation imposed by the federal antitrust laws on schemes of self-regulation within an industry, see Silver v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court cautioned that such schemes will be closely scrutinized because of their potential effect on competition within the industry. *See generally* G. Lamb & S. Kittelle, Trade Association Law and Practice §§ 11.1–9 (1956); Baum, *Self-Regulation and Antitrust: Suppression of Deceptive Advertising by the Publishing Media*, 12 Syracuse L. Rev. 289 (1961); Rockefeller, *Industry, Efforts at Self-regulation*, 10 Antitrust Bull. 555 (1965); *Developments in the Law—Deceptive Advertising*, 90 Harv. L. Rev. 1005, 1159–63 (1967).

[55] Such a procedure would afford roughly the same right to comment as is now granted by section 4 of the Administrative Procedure Act, 5 U.S.C. § 553 (Supp. IV, 1969), which provides for the filing of written comments, after appropriate notice, in the case of administrative agency rule making.

[56] The author has deliberately refrained at this time from suggesting what government agency should undertake this function. The FCC, with its broad expertise in the communications field, might be the most logical candidate. Perhaps a new agency under the Department of Commerce might best do the job. In any event, the Congress, in selecting or creating the agency to do the job, should take meticulous care to assure that the agency and the whole regulatory scheme will work in tandem with a well defined national communications policy, as well as in furtherance of national policy in the privacy area. *See generally* Miller 1236–39.

[57] *Cf.* Silvr v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court utilized the federal antitrust laws as a basis for its review of the procedural integrity of a system of industrial self-regulation.

[58] It may be appropriate to provide for binding arbitration of such disputes instead of merely conciliation. This would be feasible, however, only if the industry agency were a truly independent authority and had such status and reputation for objectivity that nonmembers of the computer service industry would regard it as a fair tribunal.

[59] *See generally* W. Gellhorn & C. Byse, Administrative Law 649–51 (4th ed. 1960). For a discussion of the utility of the conciliation process in an analogous context, see 1968 Duke L.J. 1000 (conciliation procedure in an Equal Employment Opportunity Commission proceeding).

[60] Theft of a computer program might be ground for such expulsion. In at least one case, a court has held that computer programs are "property" subject to "theft" under state law, and an employee of a computer company who stole such programs was guilty of felony theft. Hancock v. State, 402 W. 2d 966 (Tex. Crim. App. 1966).

[61] To reiterate, there should be no statutory exemption from liability in the case of voluntary and deliberate acts by the computer service company including companies offering computerized information services. At least as this author now envisions the proposed industry association, it would not deal with criteria for the voluntary release of information to "interested persons," government agencies, or other individuals, groups, or organizations. It may well be that, as the system develops and considerable experience is gained with the arrangement proposed in this article, it will eventually be appropriate for the industry association to promulgate standards governing the voluntary disclosure of information. Of course, to be really effective, especially against the federal government itself, the association should have specific federal statutory authority to promulgate and enforce such standards, and the statute should expressly make them applicable to governmental agencies.

[62] For example, three excellent papers summarizing some of the problems involved in achieving privacy and security of data in multi-programmed computer systems were presented at the 1967 Spring Joint Computer Conference. Proceedings, Spring Joint Computer Conference 279–90 (1967). The individual articles were Peters, *Security Considerations in a Multi-Programmed Computer System*, *id.* at 283; Ware, *Security and Privacy in Computer Systems*, *id.* at 279; Ware, *Security and Privacy: Similarities and Differences*, *id.* at 287. The terms "security" and "privacy" are used in special senses in those papers, as summarized by Willis Ware in the last-cited paper: "For the purposes of this paper we will use the term 'security' when speaking about computer systems which handle classified defense information which nonetheless must be protected because it is in some respect

sensitive." *Id.* The term "security" has been used in a broader sense throughout this article.

[63] *See, e.g.*, Response of United States Department of Justice (Mar. 5, 1968), filed in Computer Inquiry, FCC Docket No. 16,979.

[64] *See* Irwin, *supra* note 49, at 360–61 (1969); Miller 1099–1103.

[65] However, if the carriers utilize separate subsidiaries to engage in computer service operations which would be subject to regulation by the industry association if performed by computer companies not related to communications common carriers, such carriers or their computer service subsidiaries should be subject to industry regulation in the privacy area.

[66] Even if the FCC might be able to act pursuant to its existing general powers under the Communications Act of 1934, 47 U.S.C. §§ 151–609 (1964), there may be considerable advantage in spelling out the FCC's jurisdiction in this situation and perhaps providing for special streamlined procedures.

If the FCC is to become involved in a significant way in this situation, perhaps it should be the agency to review actions of the computer industry agency although Congress might wish to consider other alternatives before determining whether to give such jurisdiction to the FCC. See note 56 *supra* and accompanying text.

[67] This description of the NASD and its activities is taken from the 1968 NASD President's Report, 1968 NASD Ann. President's Rep. Of interest to the computer industry in formulating its system of self-regulation might be the NASD's statement of purposes:

(1) To promote . . . the investment . . . and securities business, to standardize its principles and practices, to promote . . . high standards of commercial honor, and to . . . promote among members observance of Federal and State securities laws;

(2) To provide a medium through which its membership may . . . consult, and cooperate with governmental and other agencies in the solution of problems affecting investors, the public, and [this business] . . .;

(3) To adopt . . . and enforce rules of fair practice [in the securities business] . . . and in general to promote just and equitable principles of trade for the protection of investors;

(4) To promote self-discipline among members, and to investigate and adjust grievances between the public and members . . . CCH NASD Manual ¶ 1003.

With some slight change in terminology, many of these statements might be substantially adopted by the computer industry.

[From the Congressional Record, Senate, Oct. 10, 1972]

INTERNATIONAL DECLARATION OF PRINCIPLE ON COMPUTERS AND PRIVACY

Mr. ERVIN. Mr. President, for many years the Constitutional Rights Subcommittee has been studying the impact of computers and Government data collection on individual rights and privacy. The subcommittee's studies have resulted in a series of hearings, recently published, entitled "Federal Data Banks, Computers, and the Bill of Rights." It was at those hearings that the subcommittee, among other issues, investigated the Army surveillance program.

The hearings attracted an extraordinary amount of public interest. Since that time it is clear that the public is beginning to focus on the potential dangers to individual privacy posed by the introduction of new technologies to aid Government in its insatiable curiosity for information about citizens. It is illustrative of this public concern that the platforms of both major parties this year take stands which recognize the issue and promise steps to prevent unwarranted invasions of privacy by Government data banking.

"Computers and privacy" is not only an issue to Americans. Other Western countries also see that computers can have a profound impact on economic, social, and political conditions, and that they can disturb the existing relationship between Government and citizen to the detriment of individual freedom.

In recognition of these potential consequences, a French foundation, L'Institut De La Vie—or, the Institute of Life—scheduled a conference on "Man and the Computer" last month in Bordeaux, France. The institute is dedicated to insuring that the science and technology are used for the benefit of mankind.

The institute's Conference on Man and the Computer, its second, was particularly concerned with the impact of computers on individuals. The Conference brought together over 150 experts in medicine, law, sociology, government, law enforcement, industry, communications, education, and other fields from over 22 countries, including 14 nations from Western Europe, plus Turkey, Algeria, Mexico, Israel, Canada, and even Yugoslavia, Japan, and the Soviet Union. Five special reports were prepared—on education, medicine, urban affairs, planning, and on individual life. Among the noteworthy results of the Conference was a declaration of principle on fundamental human rights. The declaration of principle stresses first of all the individual's right to privacy. In its words:

"*The Right to Privacy.* We believe that there is an interest shared by all people to have some control over the information that is collected, stored, and circulated about them. We believe it essential that consideration of this issue be an integral part of the creation of any information system."

A second right, and one which is not underlined in the United States as often as it should be, is the right to information. Since information can be considered a resource, the monopolization of information is to be avoided just as we prohibit monopolization of any other natural resource.

The declaration outlines a series of operating principles which should be observed in the creation of every computer data bank. These six principles are:

"The need to determine whether information to be collected is relevant to the purpose for which it is sought and whether it is required to be collected at all;

"The need to give the individual notice of and access to information stored about him;

"The need to limit information systems to specific uses;

"The need to regulate the use and transfer of information in such systems;

"The need to check and update information contained in these systems, supervise operation of the systems, and monitor their expansion into new areas or enlarged data-sharing operations; and

"The need for sanctions to enforce the safeguards established."

Finally, the declaration recognizes that in order to effectuate these principles, there must be first, acceptance on the part of those who operate data banks of the rights to privacy and to information; second, full public knowledge and review of all important aspects of every record system by a public authority charged especially with protecting individual rights; and third, the creation of a forum for the resolution of individual complaints arising from these systems.

This declaration of principle is unique not only because it states in clear, simple and moving terms the rights which are clear to every American, but because it demonstrates the universality of the concern for privacy. It is noteworthy that this declaration of principle was drafted by a group with widely divergent cultural and political traditions. Yet the result is one which can serve as a guide for the United States in its treatment of the problems of computers and privacy.

I ask unanimous consent that the declaration of principle adopted by the Institute De La Vie at its Conference on Man and Computer be printed in the Record.

There being no objection, the declaration was ordered to be printed in the Record.

[The dedication follows:]

CONCLUSIONS AND RECOMMENDATIONS

Presented at the final session of La Conference Internationale, "L'Homme et L'Informatique", L'Institut de la Vie, Bordeaux, France, 16 September, 1972.

DECLARATION OF PRINCIPLE

We believe that there are fundamental human rights which deserve reaffirmation in the comuuter age. It is not that threats to human rights are new in the computer age but rather that the computer is changing the economics and nature of the information processing systems of society in ways that could lead to increased encroachments on these rights. In reaffirming these rights, we do so with the hope that by making the possible opportunities and dangers more visible, the use of computer technology will result n the enhancement of these rights rather than their diminution.

Among these rights are the following:

The Right to Privacy. We believe that there is an interest shared by all people to have some control over the information that is collected, stored, and circulated about them. We believe it essential that consideration of this issue be an integral part of the creation of any information system.

The Right to Information. We believe that information gathered and stored in computers wil become as important a resource as any man has sought to employ. In each country there needs to be an integrated national policy on the availability of this resource. We believe that the individual has a fundamental human right to have access to information, not only about himself, but about his community and government and other things that impact upon his life.

At the same time, we recognize that the individual's right to privacy can conflict with society's right to know and use information. Similarly, the right to informaton of one individual can conflict with the right to privacy of another. The balance to be struck between these conflicting interests will depend on the setting, the nature of the information, and the use to be made of it. The ultimate

accommodation of interests will vary from culture to culture and country to country as values differ.

In developing information systems, we believe the following principles should be among those considered:

The need to determine whether information to be collected is relevant to the purpose for which it is sought and whether it is required to be collected at all

The need to give the individual notice of and access to information stored about him contained

The need to limit information systems to specific uses

The need to regulate the use and transfer of information in such systems

The need to check and update information contained in these systems, supervise operation of the systems, and monitor their expansion into new areas or enlarged data-sharing operations

The need for sanctions to enforce the safeguards established.

To transform these principles into operation requires

The creation of a consciousness on the part of managers of record systems about the rights of privacy and access to information

A process of public review of the goals, organization, procedures, and safeguards of record systems, preferably by a legislative body or administrative authority charged with insuring full consideration of the issues of individual rights

An appropriate forum, judicial or administrative, before which individuals can bring complaints in particular cases.

We believe that the capabilities of computer technology can and should be taken full advantage of in the design of the protective mechanisms we have recommended. Once these measures have been taken, we look toward the fruitful use of information systems to help governments and private organizations carry out the responsibilities for public policy and social progress with which they are charged. The principle we recommend should lead to the growth of greater public trust in the use of properly controlled information systems. Without this trust, the benefits of information systems cannot be realized in democratic societies.

We view the evolution of legally enforcable rights and effective remedies as being as important for the future application of computer technology as the successfull development of the technology itself.

[From the Congressional Record, June 17, 1974]

THREAT TO PRIVACY

(By Senator Charles H. Percy of Illinois)

Mr. PERCY. Mr. President, on Tuesday morning, the Government Operations Committee, in conjunction with the Constitutional Rights Subcommittee will begin hearings on a subject of critical importance to every American: personal privacy.

The focus for our hearings is a bill introduced by the Committee's distinguished Chairman Senator Ervin, Senator Muskie and myself to establish every American's right to keep personal information private and to safeguard that right with criminal and civil protections.

The bill is companion to one introduced in the House by Congressman Barry Goldwater, Jr. and Congressman Edward Koch, whose efforts I commend. It is the result of a deepening public concern about privacy invasions. These invasions are fast becoming the rule—not the exception—in American life.

The burgeoning abuse of the right of individual privacy results partly from a greatly increased capability of even a moderately endowed private or public organization to obtain, store and use vast quantities of information about people. This phenomenal technical information-handling ability is abetted by the absence of regulation (except in the area of credit information). The result is a tremendously increased potential for damaging misuse of personal information—data that the person under scrutiny does not know is so readily available.

But even more important is the startling, ominous propensity of an increasingly powerful government to use information in ways that hurt individuals direct and dramatically.

In Mendham, New Jersey, a young high school student, at the suggestion of her social studies teacher, wrote the Young Socialist Alliance in New York City

asking for information. Several weeks later an FBI agent visited the school's principal and other people who knew Lori Paton, to make inquiries about her. The FBI made a "notation" in its files about Miss Paton's innocent inquiry, and its agents wrote a memorandum for FBI files recording their "investigation" of Miss Paton. The FBI claimed that its knowledge of the student's inquiry was obtained from surveillance on all incoming mail to the Young Socialist Alliance. Under the law, such a "mail watch" is legal if it does not delay the mail and if it is confined only to data drawn from the outside of the envelope. The critical issue here is the potential lifetime damage to the reputation and career of a completely innocent teenage girl about whom an FBI "notation" and "memorandum" will always exist, unless she succeeds in having it expunged from the files of the FBI.

This is an example drawn from the more normal course of events. The FBI must make hundreds, perhaps thousands of such "notations" (we regrettably cannot know) each week.

POLITICIZATION OF THE IRS

What about malicious, politically-motivated invasion of the right of privacy? One of the most insidious abuses is attempted use of Internal Revenue Service data for political purposes.

Certain member of the present Administration at the outset of tis first term, made strong efforts to make the Internal Revenue Service "politically responsive."

A memorandum from White House aide, Tom Charles Huston to the Assistant to the Commissioner of the IRS of August 14, 1970 refers to a July 1, 1969 White House request that IRS review the operations of "Ideological Organizations." Huston's August 14 memo asked IRS to report on its implementation of that request. The IRS response, signed by then IRS Commissioner Randolph Thrower and dated September 19, 1970, explains the operations of a so-called "Special Service Group" that had been established in IRS to monitor the tax status of "organizations and individuals promoting extremist views and philosophies." Thrower's rationale for creation of that outfit was that it was necessary "to avoid allegation that extremist organizations ignore taxing statutes with impunity." Mr. Thrower's September 1970 report indicated that by then approximately 1,025 organizations and 4,300 individuals had already been examined by the IRS.

On September 21, Huston wrote to Assistant to the President, H. R. Haldeman indicating strong *dissatisfaction* with IRS action on the President's July 1969 request. He noted then that "What we cannot do in a courtroom via criminal prosecutions to curtail the activities of some of these groups, IRS could do by administrative action."

Subsequently, an undated "IRS Talking Paper" was developed, outlining, from the perspective of the White House, the case against the IRS and its lack of political responsiveness. The document suggests that "Walters (who succeeded Thrower) must be made to know that discreet political actions and investigations on behalf of the Administration are a firm requirement and responsibility on his part." Another suggestion of the "talking Paper" is that Counsel to the President, John Dean, should have "assurance that Walters will get the job done."

On June 12, 1972, Charles Colson, Special Counsel to the President, wrote Dean asking for an IRS check on Harold J. Gibbons, a Teamsters Union Vice President in St. Louis, whom Colson described as a "McGovernite, ardently anti-Nixon." This document would suggest that a connection between Dean and IRS had indeed been established and that IRS had become more "politically sensitive" in the manner outlined in the "IRS Talking Paper."

It is unclear whether there is evidence showing that the IRS did become politically responsive in a manner demanded by the White House. However, we do know that the issue was pressed.

The Joint Committee on Internal Revenue Taxation, which has direct oversight over the IRS, has filed an interim report on its investigation of the matter. This report shows that the subjects of special audits and investigations have not been treated more harshly than other taxpayers. But the Joint Committee was denied access to files of the Special Service Group. This renders the Joint Committee's study virtually useless. But, the fact that the politicizing of the IRS was attempted is beyond doubt.

The success of the effort to compromise this key agency's integrity is still in question. But the central question is not the attempt to politicize this agency—dreadful as that is. It is the doubt created in the minds of the American people—

justifiable concern that information of an extremely personal nature—might be made available to other agencies, including the White House, for political purposes.

The bill I have introduced with Senator Ervin to establish and protect personal privacy rights would remedy such abuses.

In the case of the Mendham High School student, the bill would provide her and her parents with ready access to the FBI files about her. She would have the right to examine the records and prove, if she can, the incorrectness of anything in her file. A correcting statement would be added to her file.

To eliminate politically motivated punishment by the government, the bill would require the IRS to make notations of each instance in which a file was made available to another government organization or outside person, not having regular access authority. A record of such accession or transfer must be kept.

The privacy right that S. 3418 establishes for individuals is comprehensive.

It establishes the right of a citizen to be informed whether he or she is the subject of private organization or government files. If the bill passes, in two years each individual must be told that he or she is the subject of a data file. At any other time that an individual asks, he must be informed of the fact that he is a "data subject".

The bill establishes the right to inspect all personal information contained in one's file, to learn the nature and sources of the data, and the identity of each recipient of personal data.

The bill establishes the right of every data subject to challenge, correct, or explain personal information, to demand an investigation of disputed information, to demand purging of inaccurate information and to include a 200-word personal correction of one's file.

The bill establishes the right to be informed and to give or withhold consent before personal data is given to anyone not having "regular access authority." It establishes the right to be apprised of the intended use of information and the consequences of giving or not giving permission.

The bill establishes the right to have one's name removed upon request from any organization's mailing lists. The purpose of this section is to protect citizens from unwarranted harassment.

S. 3418 defines standards for the collection, use and disclosure of personal information by government and private organizations. These standards include the following:

Personal information collection is limited to what is necessary for a "proper" function of an organization.

Information should be collected from the individual himself whenever possible.

Categories of confidentiality must be established, with various levels of controlled access to information.

Data files must be policed for accuracy, completeness and pertinence by the organization maintaining them.

The organization must maintain a list of users having regular access authority.

A complete record of the purposes of every access to any personal information in a system, including the identity of the special access user, must be kept.

Personal information must never be disclosed without specifying security requirements (e.g., the level of confidentiality), and obtaining reasonable assurance that those requirements will be observed.

No personal information concerning political or religious beliefs or activities should be collected if it will be put into a government-operated information system.

Income data shoud not be keyed to zip codes or postal districts.

Federal agencies are prohibited from requiring disclosure of personal data or requesting voluntary disclosure unless authorized by law.

The bill establishes a five member Federal Privacy Board that can make and enforce privacy rules for personal data files. The Board is required to establish an annual directory of every personal data system in the country; it is empowered to ensure that standards are met and to assist organizations to comply with privacy safeguards. It can make site visits, compel production of documents, hold hearings on violations, issue cease and desist orders, delegate authority to states and hold open hearings on exemptions. It is required to report annually to Congress.

S. 3418 is an excellent beginning for hearings and for the legislative process, and we in the Government Operations Committee will prepare this bill very carefully but expeditiously for floor action during this session.

PROBLEM AREAS

Mr. President, as you know, there are many other bills pending in this body regarding individual privacy. Without exception, they all raise problems in the minds of those of us who want to correct the present lack of controls over personal data.

Our bill is itself not free of flaws; yet, in the give-and-take of the committee room, it can be perfected. Let me cite some of the difficulties in the legislation.

The bill does not establish a mechanism to inform people as new files about them are created. The right to inspect and challenge personal files is amost meaningless if an individual does not know that a file even exists. Perhaps we should provide that people be notified whenever they become a subject of a new data file.

Another problem is that no limits have been placed on rights to inspect and challenge personal files and to demand investigations of disputed information, and no protection against excessive demands is afforded to organizations keeping data files.

For example, it would be unfair to allow a person to inspect his file every week.

As I noted, the bill requires that information should be collected from the individual himself wherever possible. This is an important provision, since it attempts to assure that the information that is collected is accurate. However, there is a possibility for abuse. If personal information is actually collected directly from the subject in every case practicable, the resulting harrassment of individuals may undo the value of the rule by creating another type of violation of personal privacy.

The requirement in the bill that *every* access to personal data be accurately recorded is unprecedented and very likely would be staggering in scope. There seems to be the unwarranted assumption that thousands of different organizations will independently and correctly establish new standard operating procedures for handling personal information. The implicit administrative burden on government and private organizations is a matter for concern and further consideration. It may be that it is possible to make a number of distinctions that will lessen the burden on organizations, yet establish basic privacy guarantees. One possible distinction is to differentiate among the kinds of organizations maintaining data. My legal staff is now working on that difficulty.

The bill provides for a Federal Privacy Board, which would be an independent agency in the Executive Branch consisting of five members designated by the President and confirmed by the Senate. There is a good deal of doubt about the validity of such an organization. It may well be that the simplest, and ultimately the best, solution is to establish rights which individuals may pursue through the judicial process, without creation of any new agency to "police" the new privacy guarantees. Or, the Privacy Board's functions could be lodged in an existing Executive branch organizataion. Or, they could be lodged in one of the existing independent regulatory commissions, or in an agency of the Legislative Branch, such as the General Accounting Office. These are some of the concerns and some of the options we must explore during our hearings.

There are other legitimate concerns. One of them is the exemption provided in the bill for national security. Personal data systems directly related to the security of the U.S. would be free from the guarantees of the act. Any federal agency could use that protection. This could permit federal agencies to abuse that cloak of secrecy, thus diminishing the intentions of this legislation.

I cite a concrete example which indicates a need for a careful, tight definition of this national security exemption.

The United States Army has been used to spy on the political activities of American civilians in Western Europe. In August, 1972, U.S. Army Military Intelligence personnel were assigned to monitor the political campaign activities of supporters of Senator George McGovern in Western Europe. The reports filed by these agencies describe the political activities of a group known as "Americans for McGovern", in Berlin. Army Intelligence reports describe their organizational meetings, leaflet distributions, announcements and local publications, ties to the official Democratic party, and even the name of a man who received an autographed picture of Senator McGovern.

Military intelligence reports describe in detail the position of McGovern supporters on issues such as tax reform, welfare reform, Federal aid to schools, equal educational opportunities, racial and sexual discrimination, national health insurance, abortion and abolition of the electoral college.

Military intelligence reports list the names of McGovern supporters, including information on their date and place of birth, marital status, passport number, occupation and residence in Western Europe.

A chart was prepared by the U.S. Army for training manuals to be used in the training of intelligence personnel in Western Europe. One such chart shows the "link" between the Democratic Party in the U.S. and the Communist Party.

Army personnel also opened the mail of American civilians in Europe. One intelligence officer has said that the Army maintains a room approximately 15 ft. x 20 ft. containing file cabinets filled with photocopies of mail of American civilians. In these files is a letter from the library of the College of Charleston, South Carolina, to a publication in Western Europe run by American civilians. The Army has photographed an index card, photographed both sides of the envelope and photographed the contents of the letter. This opening of American civilian mail occurred in June of 1973, which date appears at the top of the Army document. The Army has systematically opened the mail of the Lawyers Military Defense Committee, which is an affiliate of the American Civil Liberties Union, and a well-publicized suit against the Army in the U.S. District Court of the District of Columbia by the L.M.D.C. and other plaintiffs is contesting these privacy invasions conducted in the name of "national defense."

Other Army activities include infiltration, photographing and wiretaps.

With respect to photography, American students in Western Europe have been photographed pamphleteering for McGovern by military intelligence officials and photographs have been obtained of political petitions showing the names of American civilians who have signed the same.

The Army has collected leaflets disseminated by American civilians which describe President Nixon's involvement in Watergate. On the back of each leaflet is a physical description of the person handing out the document.

All of these activities are undertaken in the name of "national security". Such a grossly distorted use of this catch all pretext to so blatantly abuse the rights of American citizens is unwarranted, and Federal privacy law must be enacted to bring such abuses to an end. For this reason, I believe we must carefully narrow the national security exemption in this bill.

MEDICAL RECORDS ABUSE

In yet another area of personal data, almost unnoticed by the public, there is a growing assault upon the confidentiality of personal health and medical records. Information that we provide to our doctors in the intimacy of their offices frequently finds its way to insurance companies, credit files and employment records without our knowledge or approval. The improper procurement and use of medical information has had devastating effects upon unsuspecting individuals. Marriages have been ruined and reputations have been destroyed.

I would like to refer to several case histories provided by Dr. Elmer R. Gabrielli, Chairman of the Joint Task Force Group on Ethical Health Data Centers at the State University of New York. These cases illustrate the need for Federal legislation to prevent flagrant breaches of confidentiality of medical information. In one recent example, a District Attorney from a great American city was hospitalized with a serious medical condition. On the day following his hospitalization, the local newspaper in his community printed his medical records word for word.

A second, even more serious example offered by Dr. Gabrielli, involved an employee of a large defense contractor who sought reimbursement for psychiatric treatment from his company's health insurance plan. In the process of the claim, the insurance company passed on the diagnosis of the employee to his employer who in turn, passed on the diagnosis to the Defense Department. The Department initiated an investigation of the employee. Department of Defense investigators asked insinuating questions of the man's neighbors. The damage had been done.

In another case, a young woman attempted to commit suicide and subsequently received psychiatric treatment at a hospital. She was shocked to learn the details of her diagnosis, not from her doctor, but from her employer. Her employer had obtained the information from the company's health insurance agent, who had gained access to these supposedly confidential hospital records. The shock to this woman upon hearing her psychiatric diagnosis from her employer must have been intense. It calls to our attention once again the imperative need for legislation to establish limits on access to personal data. This

can be done by empowering each individual with control over who can view his personal files. The strict confidentiality of personally sensitive medical and health records clearly requires more than good faith and integrity on the part of health care personnel. It deserves and requires legal protection.

SCHOOL RECORD ABUSES

I wish to refer to yet another sensitive area in which privacy rights have been ignored and for which legislative safeguards are needed: school records. Particularly in these days when our public schools are so much in need of Federal support, the informational requirements for evaluation of Federal school aid programs can and do pose serious threats to the privacy of personal student information.

In Illinois, the League of Women Voters conducted extensive surveys of personal information systems. A study of seventy-one schools revealed that many teachers were not impressed with the need to protect personal student information. They found further that there were no standards of confidentiality imposed on faculty and staff. Clearly, a privacy problem exists, since although no school administrator in the League's survey reported giving information on students to local police, several police departments listed schools as sources for personal student data.

A Los Angeles *Times* article of October 15, 1973, "Keeping Files on 'Predelinquents' Stirs Criticism", explains that for thousands of children judged to be predelinquents (youngsters whom school authorities believe have criminal tendencies), extensive, often permanent records are kept of their participation in Federally funded community programs designed to reshape behavior. The files contain case histories, anecdotes about class behavior, reports on academic progress. The reports come from principals, teachers, parents and the counselors—some professionals, some volunteers—who work with children in the program. Many of the programs, according to a California Joint Legislative Audit Committee looking into this area, are administered through the probation departments, which keep records after the pilot predelinquency programs end. The article said that this "creates the possibility that the records will be used for probation purposes." Because these programs are operated by law enforcement agencies, "voluntary" participation by schools is inherently coercive, and there is the danger that participating children will be treated as future criminals.

In California, some state officials say the programs' procedures violate the children's civil rights. In the juvenile court system, the same children would get protection of due process, presumption of innocence and right to counsel. There are no such protections in the voluntary programs. For example, there are no provisions for destruction of indidivual records after the programs are terminated. On the other hand, most juvenile arrest records are sealed. State and Federal officials administering such programs justify the data storage by maintaining that a juvenile risks his privacy in return for the benefit derived from the program.

Walter Quinn, California's then acting deputy auditor general, defended the practice of keeping the files open, saying:

"We think it may be fairly stated that the benefit accruing to a juvenile by being in one of the voluntary programs is paid for by foregoing certain rights to which he is otherwise entitled."

This sort of blanket judgment, that would attempt to justify the disregard of students' privacy, is wholly inappropriate. The principal at Glenknoll Drive Elementary School in Yorba Linda, California, has stated that school teachers and administrators are about 75% right in their designations of youths as predelinquent. Not only are such claims unverifiable and therefore suspect, but I wonder about the other estimated 25% of those youths who are falsely labeled predelinquent. It is they who will suffer without any reason from the stigma of such a label.

Dr. Carl Marburger, spokesman for the National Committee of Citizens in Education, characterized the absence of controls over personal school data as "generally an ungoverned and unsupervised system." "Anyone," he said, "even the school secretary, can put something into the record." No one knows precisely what goes in and parents are often denied access to what is in the record.

The Illinois League of Women Voters survey indicated that most schools do not allow parents to challenge the accuracy and contents of their children's school records. In a majority of cases, parents are not even allowed to see their children's school files. Frequently they must be satisfied with interpretations and comments offered by school counselors. Yet those same files are accessible to police, university researchers and even other students working for the school administration.

This situation represents an intolerable abuse of the informal privacy rights of students and parents. Dr. Marburger's assessment is indeed frightening. As he say, the American school sytem maintains "the most vastly comprehensive data operation of any institution in the country. If you have a child in school, there is a dossier which sometimes contains inaccurate and potentially damaging information."

We cannot allow our children's privacy, and our privacy as parents, to remain unprotected. We must not let indiscriminate notations in school files go unchallenged. We must not allow these files to be available to anyone other than authorized school personnel. In the rare instances in which others have a need for such information, parents and children must be informed, and access should require either their consent or a court order. These protections can and will be afforded.

POTENTIAL CABLE TELEVISION ABUSES

Looking toward the future, the rapid advance of technology continues to give rise to new threats against individual privacy which must be anticipated. I offer just one example: developments in the advancing field of cable television. Cable stations across this country are acquiring capabilities for broadcasting as many as 40 or 50 channels. Citizens will increasingly be offered a large variety of television programs that have been tailored to their individual tastes and preferences. As this possibility is being realized, cable television companies are experimenting with techniques for monitoring the viewing habits of individuals.

Simple tabulations of the number of people who watch particular programs, thus enabling cable television operators to make accurate programming decision, could be accomplished *without* compromising the privacy of individual viewers. But cable systems in a number of cities, including Rossmoor's Leisure World Retirement Community in Mesa, Arizona, and experimental systems like TOCOM (Total Communications) in Irving, Texas and Theta-Com in El Segundo, California, routinely and automatically monitor program choices and viewing habits of individual cable television subscribers. Viewers have no choice and cannot exercise any control over such monitoring.

There is now no national law that would forbid a cable station from telling anyone about the individual tastes of each and every one of its subscribers. A business, so notified, is free to bombard the unwitting cable subscriber with any number of sales pitches based on what is known about the viewers personal entertainment tastes.

Thus, in the not too distant future, computer-aided records of the programs an individual watches can be analyzed for their commercial, political or scientific research value. Preparation of viewer files would establish what is essentially a cultural taste data bank and thereby create an opportunity for access and abuse of personal information that does not now exist.

The technological capacity to invade the privacy of our homes to acquire such information gives frightening substance to the fiction of Big Brother, from George Orwell's *1984*. Perhaps such monitoring systems should never be established at all. But if they are established, we must ensure that they operate only with the knowledge and explicit consent of the "watched".

Certainly, this example is somewhat futuristic. However, it suggests that we must maintain a vigilant attitude toward new and unregulated technologies if personal privacy is to be protected.

CONCLUSION

Mr. President, all of these examples that I have mentioned suggest the need for strong measures to support the right of privacy. The legislation which Mr. Ervin, Mr. Muskie and I have introduced provides a good base for final legislation. It will reach information systems and data files across the country and make secure a sacred personal liberty.

STATEMENTS BY MEMBERS OF THE HOUSE OF REPRESENTATIVES ON PRIVACY, SUBMITTED BY CONGRESSMAN KOCH AS EXHIBIT AT HEARING, JUNE 18, 1974

[From the Congressional Record, House, April 2, 1974]

CONGRESSIONAL COMMITMENT TO PRIVACY

The SPEAKER. Under a previous order of the House, the gentleman from California (Mr Goldwater) is recognized for 60 minutes.

Mr. GOLDWATER. Mr. Speaker, the preservation of the rights of privacy of all Americans is a vital national issue. We have called this special order to serve notice that Congress intends to act to restore this personal liberty of all our citizens. The collectors of information must be held to high standards to insure against abuse. The intrusions so prevalent in this electronic age must be strictly controlled.

Joining me today as principal sponsors of this special order are the gentlemen from New York (Messrs. Koch, Horton, and Kemp), the gentleman from California (Mr. Edwards), and the gentleman from Pennsylvania (Mr. Moorhead).

We represent a bipartisan coalition diverse in our political philosophy but united in the goal of enacting right to privacy legislation.

We strive to correct the imablance now existing between the public need for information and private rights against undue collection of personal facts.

We call for an end to secrecy of personal files, for individuals to be able to inspect and correct their files, and control their use.

Mr. Speaker, I welcome my colleagues who have come to discuss privacy issues this afternoon.

Mr. Speaker, these days, applying for or renewing your drivers' license is getting like being processed by the police for a criminal offense. Almost all States require the applicant's social security number and 29 States and the District of Columbia now provide photographs on drivers' licenses. Considerable additional information is being placed in motor vehicles and drivers' license files making up small dossiers, in some cases.

One of the more onerous practices is that some 14 States, when a person is photographed for his or her license, a negative of each photograph is placed on file. The citizen is normally unaware of this practice. These negatives create a statewide file on mug shots on virtually every adult.

OPERATING STATISTICS FOR 5 LARGE INVESTIGATIVE REPORTING FIRMS

Company	Number of files, 1972	Total number of investigative reports, 1972	Insurance reports, 1972	Credit reports, 1972	Employment reports, 1972	Inspector man-years, 1972	Consumer interviews since April 1971
Retail Credit	46,000,000	13,731,049	12,537,328	152,437	1,041,284	(1)	135,662
Service Review	50,000	3,396,812	3,375,889	(2)	20,923	738	(1)
Hooper-Holmes	2,500,000	1,443,661	1,368,439	25,734	49,488	361	5,708
O'Hanlon	4,000,000	492,298	492,298	(2)	(2)	(1)	1,299
American Service Bureau	1,970,000	784,379	781,241	(2)	3,138	1,160	980
Total	54,520,000	19,848,199	18,555,195	178,171	1,114,833		

[1] Not available.
[2] Negligible.

Source: Data submitted by each firm

Laws and regulations are only part of the solution to reduce unwarranted intrutions into personal privacy. Corporations manufacturing computers, electronics and photographic equipment should exercise restraint in encouraging excessive data surveillance. I am pleased to call attention to the fact the Polaroid Corp. produces identification cards as do other firms. However, they have refused to supply equipment where they believe control rather than simply administrative requirements are intended. We need more of this corporate responsibility.

FIFTY-FOUR MILLION CREDIT FILES

Mr. Speaker, the volume of credit files in active use in the United States is staggering. According to recent statistics, each of the five largest investigatory reporting firms has an additional 37 million reports on these and other individuals. When we hear the statement "there is a record on you," we seldom need to challenge it. But we must begin asking how many such records are kept, where they are located, and what they contain. I have proposed legislation to permit these questions to be answered for every person about whom records are maintained.

The following table clearly demonstrates the scope of information on hand in but one area of recordkeeping.

COMPLAINTS ABOUT THE SOCIAL SECURITY NUMBER

Mr. Speaker, public opposition to the social security number being used as a universal identifier is deeply felt by a great many Americans. Commercial and government interests which go blithely along demanding a person's number on every type of transaction are only asking for a public hostility which will soon overturn these practices.

I am not against the use of identification numbers on bank accounts, student records, or any other occasion where this will serve to separate different files, expedite transactions, and raise the level of accuracy. However, the social security account number was never intended for that purpose. It is the identification number for people's pension system. I have sponsored legislation to disallow this number for any purpose but that called for by statute. Let the people's dignity be restored by abandoning once and for all this practice.

To illustrate personal feelings over the use of the social security number let me include actual quotations from letters I have received from persons living in 15 different States.

"The state of Pennsylvania is going to have this (SS) number on our drivers license and hunting license starting next year . . . this is frightening, 1984 is here . . .

"The hassle that is incurred upon me with SS bothers me the most. Many places won't cash your check without your SS number . . . you purchase stock, they want your SS number . . . you open a bank account, they want your SS number . . . you rent a car . . .

"I resent the need for me to put this (SS) number on my physical for the FAA.

"It seems everytime I turn around I am asked for my SS number . . . the bureaus both state and federal want it for boat ownership (federal documentation), auto driver's licenses, applications for Mississippi state auto tags, etc. etc.

"You are on the right track . . . I am 43 years old and I have always prided myself on paying my bills and being honest and truthful. I recently had to go to a lot of trouble to get a bad credit report removed from my name because I had an argument with a merchant over a $16.00 bill for bad merchandise. It was only through the help of a man in the Retail Credit Assn. that I was able to do this, and I was cleared . . . isn't that one hell of a set of circumstances to have to get together to clear a bad credit report for $16 when I have money in savings certificates.

"The last time I registered to vote (with the Women's League of Voters) on the registration slip there was a space for the SS number . . . the very thought that SS should even be linked up to voting is a disturbing thought.

"For some time, many I know, and myself, have been worried about that situation and having to use the SS number on all documents. Germany and Russia started that way to gain control of everyone and everything they did.

"There are very few, if any, persons who have not at one time or another been victimized by information obtained from computer banks . . . you have my full support.

"Seems we can't even save a few dollars now and then without some spy telling the information to a credit reporting agency and they in turn publish the information in printed form and mail to other subscribers. This in turn fires up the promoters who would like to talk us out of the last dollar we've got.

"The overzealous efforts of those who insist upon making hay out of credit information—it even extends to telephone directory publishing companies and

those publishing city directories, who lease lists of addresses to businesses and finance companies—have become a nightmare for the average private citizen.

"There is almost no privacy left now. When I enrolled at the LA Valley College in Van Nuys, would you believe on one of their forms they gave you to fill out they asked if you took the pill, had hot flashes . . . and about 20 more questions just as personal and NONE OF THEIR BUSINESS. Now, they want our medical records to be available to HEW . . .

"As files expand and becomes interconnected through various communication links, the possibilities for unauthorized access will surely grow.

"I am a computer system analyst with 18 years of continual professional involvement in data processing . . . the updating of computer-stored arrest record is no different than the updating of a name and address file. Unfortunately, most systems developed during the past 20 years have been unable to update records rapidly, accurately or even efficiently. There is little doubt in my mind that a person once entered into the Criminal History File would be, and remain for all time, as "guilty as he ever was, or worse yet, might be.

"My mother is elderly, living in Illinois, and thinks that she must have her SS number tattooed on her brow.

"I believe that in another year each person's toilet tissue will have to bear his SS number so that the government will be able to compute how many times a year the individual flushes his toilet!"

Mr. KOCH. Mr. Speaker, will the gentleman yield?

Mr. GOLDWATER. I yield to the gentleman from New York.

Mr. KOCH. I thank my colleague from California for yielding.

Mr Speaker, I first want to thank the Speaker for sitting with us this afternoon at this late hour. I know that he establishes, as he has established commitments over the past, the congressional commitment for privacy. I want to thank him on behalf of the sponsors for his being with us. I am just very proud to be sponsoring with my congressional colleagues this Commitment to Privacy.

Mr. Speaker, I am very pleased to be sponsoring the congressional commitment to privacy with our colleagues, Barry Goldwater, Jr., Don Edwards, William Moorhead, Frank Horton, and Jack Kemp. And, we are honored to have you presiding during this special order. Many Members are in agreement that the area of personal privacy needs the attention of the Congress. The issue of privacy is one that transcends political partisanship and we are working together to develop ideas to help us deal with the problem in a balanced and comprehensive way. Congress must focus its attention on the massive collection of information and compilation of dossiers that are taking place. Recordkeeping, both computerized and manual, has already become a hydra-headed monster.

An individual does not really know who has the information about him, or how many agencies or corporations are using it or for what purposes. He has no mechanisms for providing explanations, or to add mitigating facts. And, most important there are no limits on what can be collected either by the Government or the private sector.

There should be a strong new disincentive for the establishment of unnecessary files on individuals. Where records are maintained, they should be treated more carefully and with more respect than presently is the case. Irrelevant, incorrect and dubious material must be weeded out.

To protect this right of privacy, I have introduced legislation in each Congress since the 91st Congress. It was 5 years ago in 1969 that I introduced the first Federal Privacy Act.

That bill pending before this Congress is H.R. 667 as amended, now known as H.R. 12206 and H.R. 12207 and it was recently the subject of hearings before the House Government Operations Committee. It responds to the problem that individuals face today in not knowing what Government agencies maintain files on them—and most important whether these files contain erroneous, irrelevant and sometimes unfairly damaging material. My Federal Privacy Act, which now has 96 cosponsors, requires that any Federal agency maintaining manual or automated records on a person, organization or corporation, permit the person to inspect his own record and have copies made at his own expense; permit the person to supplement the information contained in his own record; permit the removal of erroneous information of any kind, and provide that all agencies and persons to whom the erroneous material has been previously transferred be notified of its removal; require the notification of the person if the record is disclosed to any other agency or person not employed by the agency maintaining such record; prohibit the disclosing of information of any kind in the record to individuals in the agency other than those who need to examine the record in the per-

formance of their duties; and finally, would require the maintenance of a record of all persons inspecting such records. Exceptions would be made in the case of records required by Executive order to be withheld in the interest of the national defense and foreign policy and investigatory files compiled for criminal law enforcement purposes.

H.R. 12207, creates a Federal Privacy Board to supervise the administration of the provisions in the bill. It would permit an appeal by an individual seeking the removal of erroneous or misleading information contained in his file. The Board would also hear complaints that an agency had not complied with other requirements of the bill. The Federal Privacy Board would also establish what an agency could collect, and limit the collection to material relating to the agency.

There are presently numerous agencies collecting information about individuals—the Department of Defense, Social Security Administration, Internal Revenue Service, and the Civil Service Commission to cite a few. All kinds of information are collected: academic achievement, health, court cases, credit standing, census data, police records, birth and marriage, employment history, loyalty-security clearances, military service records, and tax returns.

Often the data is acquired by Government agencies from private sources—not necessarily using skilled investigators. The combination of fact, opinion and rumor may create a false picture. This bill would allow the individual the right to rebut any false or incomplete information which might, under ordinary circumstances, be used against him without his full knowledge.

To extend the central premise of this legislation to all computerized data banks, not just Federal data banks, I introduced with Mr. Bell, from California on August 1, 1973, H.R. 9786 to regulate the use of all computer data banks in the country. This bill will not prevent the collection of valid data either by private or governmental agencies, but will impose reasonable controls on what can be collected, or how it can be dispersed so as to protect the privacy of our citizens.

It is about time that the Federal Government establish a national policy regarding computers and computer abuses in the interests of protecting the privacy of our citizens. No amount of State legislation will insure that residents of another State will be protected. We must have Federal oversight in this matter.

Under the bill, all data banks, State, local government and private, would be required to register with the Federal Privacy Board. The Board would issue guidelines for the collection, and maintenance of information to assure that the material in a person's file is correct, current and pertinent to the approved purpose of the data system.

This bill is similar to Sweden's national law covering the operation of data banks containing personal information.

In 1971, I introduced a bill, which is H.R. 694 in this Congress, which extends the same disclosure requirements contained in H.R. 667 to the House Internal Security Committee. It requires the committee to notify persons of files maintained on them and to allow such persons to examine their files, and supplement the information in the record. An accurate record of the names and positions of all persons inspecting such records and the purposes for which the inspections were made must be maintained.

There is a special dimension to the privacy problem created when the executive branch of the Government collects information about the legislative branch. The problem emerged in 1972 when then Acting Director of the FBI, L. Patrick Gray admitted that the FBI had been maintaining files on Members of Congress. His concession came only after columnist Jack Anderson had discovered FBI files on Representatives Frelinghuysen, Reuss, Fauntroy, Speaker Albert, Ford, and others.

It has been revealed by the media that the FBI has made available files on Members of Congress and the public for the purposes of intimidation. Then New York Times on February 25 stated:

"The source recalled one Senator who had been told of an investigation concerning his daughter, a college student who had "gotten involved in demonstrations and free love," and a Republican Representative who had been told the Bureau possessed evidence indicating that he was a homosexual. "We had him in our pocket after that," the source said of the Representative. He added that he could not recall the Senator, a liberal Democrat, ever criticizing the FBI in public."

When I ascertained that the FBI had been accumulating dossiers on Members of Congress, I along with Congressmen Benjamin Rosenthal and Jonathan Bingham asked the Director of the FBI to provide us with our respective files. The FBI did not do so and so thethree of us initiated a lawsuit to compel

the opening of those files to us. Subsequent to the lawsuit, FBI Director Kelley announced he was modifying his prior refusal to make our files available to us. I have received my file which includes newspaper clippings, a flyer which lists my opposition to the ABM, my correspondence with the FBI on the subject of dossiers, my testimony against Acting Director Patrick Gray's confirmation before the Senate Judiciary Committee and a fact sheet which opened my file with the FBI when I was elected. That fact sheet is very interesting and I am setting forth the information exactly as it appears.

[The information follows:]

NOVEMBER 7, 1968.

U.S. GOVERNMENT MEMORANDUM

Mr. Bishop.
Mr. A. Jones.
Edwin I. Koch (D-New York), Congressman-elect—17th District.

DETAILS

On 11–5–68 Democrat Edwin I. Koch of New York City, was elected to the 17th Congressional District seat held by retiring Repr. Theodore R. Kupferman (R). Koch who was born in 1924 in New York City attended the College of the City of New York and received his LL.B. degree from New York University. He is a former councilman and has been a Democratic leader since 1963.

INFORMATION IN BUFILES

A check of Bureau indices reflects no reference identifiable with Koch.

RECOMMENDATION

None. For information.

If the FBI failed to ascertain correctly what my name was, it has always been Edward and never Edwin, one cannot help but speculate on what other inaccuracies its voluminous dossiers contain. There is no question that there must be limitations on the kind of information collected and how it is used. There is a balance to be maintained, however, between the need for information and the need for personal privacy. The problems have been recognized. Now we must make certain we deal with them, not with more studies, but with legislation long overdue.

I have initiated legislation, cosponsored by 21 other Members of Congress, to prohibit the FBI from maintaining files on the Congress, except where they are required in pursuit of a criminal investigation, or as part of an investigation where a Member might be appointed to the executive or judicial branch. Other than these two areas, there is no bona fide reason to maintain files on Members of Congress by the executive. And, the practice of doing so should cease. The bill would require the destruction of FBI files on Members of Congress after a period of 60 days. Each Senator and Representative would have the opportunity during the 60-day period to examine the contents of his or her file.

I would like, Mr. Speaker, at this time to discuss in greater detail one recent victory in the area of privacy. On March 22, Defense Secretary James R. Schlesinger authorized the removal of separation program numbers and reenlistment code numbers from all discharge papers. As you know, the Honorable Les Aspin from Wisconsin and I have been urging that this decision be made and we are the sponsors of legislation to effect that change. We were pleased to see that at the urging of over 50 Members of the House who were cosponsors of the bill, and through the efforts of House Armed Services Chairman F. Edward Hébert, the administration changed its policy in this matter, voiding the necessity for legislative action.

At the time of discharge, a serviceman is given a discharge paper, DD Form 214, Report of Separation from Active Duty, which contains a numerical code specifying the specific reason for release. The code, called separation program numbers—SPN's—can unfortunately penalize a veteran for life. The code numbers and what they designate, while intended to be confidential, have become publicly known. The consequent invasion of privacy may never end for a veteran with a prejudicial SPN. Employers who have been able to get copies of the number designation often use this information in an adverse way undoubtedly preventing veterans from obtaining jobs when they were either equally or better qualified than the nonveteran applicant.

The SPN numbers which appear on honorable as well as undesirable and dishonorable discharges can be pejorative. In fiscal year 1973, 35,640 servicemen who received honorable or general—under honorable conditions—discharges were also branded with a SPN marking them as unsuitable; 21,000 were identified as possessing "character and behavior disorders"; 10,000 others were labeled as suffering from "apathy, defective attitudes, and an inability to expend effort constructively," and nearly 3,000 were simply charged with "inaptitude."

Not one of these veterans was guilty of an offense under military or civilian law, and not one of them was allowed a hearing before an administrative board—nor was he permitted counsel. The SPN was in every case an arbitrary decision made by others, and the serviceman could have been completely unaware of its meaning or significance.

Under the new rules, the SPN's will be maintained in the file of the individual and releasable only at the request of the veteran.

Also, DOD regulations will provide that a veteran who would like a new discharge paper without a SPN number or reinlistment number will be able to request it from the Defense Department as a result of this new policy.

However, I feel that it is not enough to let the veteran request a new discharge certificate. A great part of the problem has to do with the fact that veterans do not know that the SPN's exist on their discharge papers. I believe that the DOD should send without a request to all those veterans discharged since the early 1950's when SPN's were instituted, updated DD forms 214–superseding the discharge paper issued when they were discharged from the service—which would not show these SPN's or reenlistment code numbers.

I have written to Defense Secretary Schlesinger urging that he comply with this suggestion. I also believe that there can be coercion on the part of employers who request that veterans authorize the release of SPN's to them. I propose that the information not be supplied to an employer or third parties even with the veteran's consent, so as to protect the veteran against undue pressure. If my colleagues in the House concur, I would urge them also to write to Secretary Schlesinger.

I originally became interested in the subject of SPN's as a result of an inquiry made by a serviceman who advised me that he was being given a discharge which would bear on it a reference to his "suspected homosexual involvement." At that time my inquiry was directed to the fact that this particular serviceman was being denied the opportunity of contesting the allegation and so I commenced the correspondence which begins with my letter of July 7, 1971. The issue developed however, so as not simply to involve this one serviceman but ultimately to involve tens of thousands of servicemen. When I sent my first letter, I did not know what a SPN number was. I do now and there can be a few victories that can provide as much satisfaction as this one, in that in a relatively short war with the Department of Defense beginning with July 7, 1971, and ending with the announcement of Defense Secretary Schlesinger on March 22, 1974, a wrong was righted and tens of thousands of veterans will benefit.

[The correspondence follows:]

HOUSE OF REPRESENTATIVES,
Washington, D.C., July 7, 1971.

Secretary MELVIN LAIRD,
Department of Defense,
Washington, D.C.

DEAR MR. SECRETARY: I have on occasion received complaints from young men in the Army who have been discharged as the result of their being homosexuals. The discharge which they receive as I understand it is often less than honorable and obviously has a chilling effect upon their personal and professional lives after they leave the service.

I would appreciate your advising me whether the barring of homosexuals in the Armed Forces is by law or by regulation, and if the type of discharge they receive, which often appears to be punitive, is by law or regulation. I would appreciate receiving your comments on this matter and informing me, if the policy is governed by regulation, whether you would consider changing those regulations so as to permit honorable discharges to those discharged for homosexual conduct.

Further, I should like your point of view on the proposal advanced by some that private homosexual conduct off the base should not bar service in the Armed Forces. Prime Minister Pierre Trudeau summed up my feelings when he said "the state has no business in the bedrooms of the nations."

Sincerely,

EDWARD I. KOCH.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., July 20, 1971.

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of July 7, 1971, regarding Department of Defense policy concerning homosexuals in the Armed Forces.

The enclosed Fact Sheet regarding Department of Defense policy on homosexuals in the Armed Forces is provided for your information. No changes are contemplated regarding this policy.

The policy regarding the type and character of administrative discharge governing the separation of homosexuals from the Armed Forces is contained in Department of Defense Directive 1332.14, "Administrative Discharges," dated December 20, 1965 [Sections VII.G 6, and 1.2]. A copy is enclosed for your information.

The nature of a discharge issued as a result of being adjudged by court-martial is specifically governed by Federal statute, 10 United States Code 925. This section encompasses all unnautral sexual intercourse between humans or between humans and animals. Some homosexual relations could come within the provisions of this section. The maximum punishment which may be imposed for a violation of Section 925 is outlined in paragraph 127c, Table of Maximum Punishment, *Manual for Courts-Martial, supra* as follows:

By force and without consent: Dishonorable Discharge, confinement at hard labor for 10 years, total forfeiture of all pay and allowances.

With a child under the age of 16 years: Dishonorable Discharge, confinement at hard labor for 20 years, total forfeiture of all pay and allowances.

Other cases: Dishonorable Discharge, confinement at hard labor for 5 years, total forfeiture of all pay and allowances.

The accused may be charged with assault with intent to commit sodomy in violation of 10 United States Code 934. The maximum punishment in violation of section 934 is a Dishonorable Discharge, confinement at hard labor for 10 years, and total forfeiture of all pay and allowances.

The *Manual for Courts-Martial* is an Executive Order of the President of the United States as prescribed by section 836, 10 United States Code. All branches of the Armed Services are bound by its provisions.

I trust that the information provided will be of assistance to you. Your interest in matters pertaining to the Military Services is appreciated.

Sincerely,

LEO E. BENADE,
Major General, USA, Deputy Assistant Secretary of Defense.

HOUSE OF REPRESENTATIVES,
Washington, D.C., August 11, 1971

Secretary MELVIN LAIRD,
Department of Defense,
Washington, D.C.

DEAR MR. SECRETARY: I am writing to you with further reference to the question of homosexuals in the Armed Services, about which I wrote to you on July 1, 1971.

While I do not approve of the Department of Defense's policy to discharge all homosexuals automatically from the military, I would like to direct this letter to change which could be made in current policy regarding the type of discharge given to homosexuals. When referring to a homosexual in this letter, I mean only a consenting adult who has engaged in homosexual acts on his or her own time and not in public.

Apparently, each branch of the service has a certain discretion in deciding how such an individual is to be discharged, and that such persons usually are not given court martials but are discharged administratively. According to existing regulations as set forth in the Department of Defense Directive No. 1332.14, December 20, 1965, a homosexual could be given administratively either an honorable (Unsuitability G–6) or undesirable (Unfitness I–2 or Misconduct J–1) discharge.

With an undesirable discharge, it is my understanding that any veteran benefits to which an individual might otherwise be entitled can be cut off at the discretion of the administering agency. Furthermore, the discharge papers are

marked "under terms other than honorable" accompanied by a code number signifying sexual deviation. This type of discharge is, in effect, a harsh, punitive measure, one that hardly reflects the contemporary and more enlightened attitude of society today towards an individual's sexual preferences.

Not only is present military policy on this matter cruelly out of date, but I believe that what little discretion exists relating to the method of discharging homosexuals is being abused. By way of illustration, I refer you to SECNAV Instruction 1900.9, April 20, 1964, which in my estimation encourages Naval personnel to give undesirable discharges to any homosexual or suspected homosexual. On the first page of this document, paragraph 4f states:

"When processing an individual by administrative action in accordance with this instruction and when the conditions prompting such action are essentially voluntary participation in aberran sexual activity, the separation of the individual will normally be characterized as having been "under conditions other than honorable." Administrative processing of cases should therefore contemplate such an ultimate disposition."

I cannot see that homosexual behavior in the military is an "offense" which merits this type of discharge. While it is apparent that the leaders of the military, in order to maintain discipline, feel it necessary to exclude homosexuals; there is no need to gratuitously punish them with an undesirable discharge.

Usually these individuals are being punished for a failure to comply with the special dictates of an artificial society which they were forced to join. Many, no doubt, were unaware of their homosexual tendencies before joining the service. Furthermore, the present policy of indicating the reason for discharge as sexual deviation constitutes an invasion of privacy. The military can, of course, keep its own records indicating why an individual was separated, but that information ought not in any way be made public.

What might be argued by some to be the concern of the military in one's personal life while an active military duty certainly ought not to be the concern of others in civilian life.

I would hope that you would give serious attention to this matter and advise me whether or not you would be willing to alter present Department of Defense policy, so that homosexuals, as defined in this letter, are given honorable discharges. Particular attention should be given to issuing new directives to supersede any documents such as SECNAV 1999.9 referred to above.

Sincerely,

EDWARD I. KOCH.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., August 19, 1971.

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of August 11, 1971, requesting that the Department of Defense alter current discharge policy so that a homosexual would be given an honorable discharge when the consenting adult engages in homosexual acts on his or her own time and not in public.

We cannot agree that Department of Defense policy concerning the discharge of homosexuals, as enumerated in my letter of July 7, 1971, is "cruelly out of date and does not reflect the contemporary and more enlightened attitude of society."

It is noted that in your reference to paragraph 4f, SECNAV Instruction 1900.9 dated April 20, 1964, the following was omitted:

"Whenever a higher character of separation is found to be warranted upon departmental review, such will be effected and command submitting case shall take pains to note all circumstances favorable to the individual which would affect the type of discharge to be awarded."

Accordingly, we do not believe this paragraph, when considering its full meaning and coupled with the total intent of the Instruction, encourages the issuance of undesirable discharges to homosexuals.

At the time a person is separated from the military service he is furnished a DD Form 214 (Armed Forces of the United States Report of Transfer or Discharge) which reflects the type of discharge, reason and authority. A separation

designator number instead of a narrative statement is used to reflect the reason for separation. This is done to afford the individual who receives a less than honorable discharge some protection from stigmatism which could result from words used to describe the reason for his discharge. The release of these separation designator numbers is closely monitored and provided only to governmental agencies indicating a "need to know." Accordingly, this information is not made a matter of public knowledge.

I trust that the information provided will be of assistance to you. Your interest in matters pertaining to the military services is appreciated.

Sincerely,

LEO E. BENADE,
Major General, USA, Deputy Assistant Secretary of Defense.

HOUSE OF REPRESENTATIVES,
Washington, D.C., January 7, 1972.

Maj. Gen. LEO E. BENADE, *USA*,
Deputy Assistant Secretary of Defense,
Department of Defense, Washington, D.C.

DEAR GENERAL BENADE: I am writing to you with further reference to the question of homosexuals in the Armed Services. I thank you for the response which you sent and which I am enclosing.

I assume from the reference to paragraph 4f, SECNAV Instruction 1900.9, that it is your intent that the Department of Defense whenever possible will provide an honorable separation as opposed to an undesirable discharge to homosexuals. I would appreciate being provided with the number of undesirable discharges issued as the result of homosexual activity each year for the last 5 years, and, if the records are available within that same period, the number of honorable discharges issued to homosexuals.

With respect to the separation designator numbers and your belief that they are not a matter of public knowledge, may I tell you that they indeed are. Employment agencies are well aware of these numbers and as I am sure are many others. What purpose does it serve to place the designator number on the discharge when that information can be kept in the file? In view of that, I would ask you to consider reviewing a change in this area.

Thank you for your interest in this matter.

Sincerely,

EDWARD I. KOCH.

DEPARTMENT OF DEFENSE—ADMINISTRATIVE DISCHARGES—HOMOSEXUAL TENDENCIES

	Honorable	General	Total
1967	64	414	478
1968	230	322	552
1969	254	192	446
1970	250	182	432
1971	204	214	418
Total	1,002	1,324	2,326

	Sexual perversion			
	Honorable	General	Undesirable	Total
1967[1]				
1968	117	294	654	1,065
1969	140	370	586	1,096
1970	119	481	419	1,019
1971	93	439	235	767
Total	469	1,584	1,894	3,947

[1] Data not available.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., January 17, 1972.

HON. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of January 7, 1972, requesting additional information on the matter of homosexuals in the Armed Forces.

The enclosed chart depicts, the administrative discharges isued for homosexual tendencies or sexual perversion during fiscal years 1967–1971.

In regard to your comment regarding separation designator numbers (SDN) being public knowledge, it is re-emphasized that the Department of Defense does not make SNDs a matter of public knowledge.

It should be noted that the purpose of DD Form 214 is threefold: (1) provides the recipient with a brief record of a term of net service during his current term of service, (2) povides various Governmental agencies with an authoritative source of information, and (3) provides the military service information for administrative purposes. The form serves a multitude of purposes and the elimination of data such as "reason for separation and authority" would drastically reduce the value and use of the document. For example, the elimination of SDNs from the data element "reason for separation and authority" on the DD Form 214 would cause a lengthy delay by the Veterans' Administration in determining an individual's eligibility for veterans' benefits inasmuch as a time-consuming search and review would have to be made of the veteran's record which is retired to the appropriate record center of the Service upon his discharge.

While the Department of Defense is committed to a periodic re-examination of policies relating to the preparation of and the inclusion of data on the DD Form 214, no changes are contemplated concerning the elimination of SDNs from the document.

I trust the information provided will be of assistance to you. Your interest in matters pertaining to the Armed Forces is appreciated.

Sincerely,

LEO E. BENADE,
Major General, USA,
Deputy Assistant Secretary of Defense.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., February 4, 1972.

HON. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of January 28, 1972 regarding homosexuals.

The administrative discharge statistics provided in my letter of January 17, 1972 represents the complete break out of data maintained by this office.

Thank you for your letter.

Sincerely,

LEO E. BENADE,
Major General, USA, Deputy Assistant Secretary of Defense.

HOUSE OF REPRESENTATIVES,
Washington, D.C., February 29, 1972.

CONGRESSIONAL LIAISON,
Department of the Navy,
Washington, D.C.

DEAR SIR: I am writing to you concerning RM3 Robert A. Martin, Jr., 157–40–7679, AF South Box 148, FPO New York 09524.

In view of the gravamen of the charges against him and what the effect of a geenral discharge given for homosexuality will have on his career in the future, I believe justice requires that he be given a court martial, as he has requested, so that he might defend himself against the charges.

It was never intended, in my judgment, to permit discharges under less than honorable conditions as a way of allowing the Navy to avoid proving charges in a serious case. He is aware of the penalties that might flow from a conviction at a court martial which are greater in degree than those from administrative proceedings, and he is willing to take his chances because he believes he is not guilty of the charges.

I would therefore appreciate your giving him the opportunity to defend himself in court and your advising me of the disposition of the matter.

Sincerely,

EDWARD I. KOCH.

HOUSE OF REPRESENTATIVES,
Washington, D.C., January 28, 1972.

Maj. Gen. LEO E. BENADE, USA,
Deputy Assistant Secretary of Defense, Department of Defense,
Washington, D.C.

DEAR GENERAL BENADE: Thank you for your letter of January 17th responding to my earlier correspondence concerning homosexuals in the Armed Services.

Because the military's definition of "sexual perversion" includes more than homosexual acts between consenting adults it is impossible for one to interpret how many of those undesirable discharges, listed in your table of administrative discharges, were for homosexual activity between consenting adults. Only a comparison of honorable, general, and undesirable discharges specifically relating to homosexual activity between consenting adults would reflect the military's present policy towards this so-called "offense." If you have such specific figures, I would appreciate receiving them.

It appears from your letters that the Department of Defense has no intention at this time of altering its present policy regarding homosexuals. While I do not want to prolong this correspondence endlessly, I do want to state that in my opinion your reason for refusing to eliminate SDN's from discharge-papers are not persuasive. If and when the Department of Defense conducts a "periodic re-examination of policy, I trust the elimination of SDN's will be approved, for indeed their meaning is public and their effects harmful.

Sincerely,

EDWARD I. KOCH.

HOUSE OF REPRESENTATIVES,
Washington, D.C., March 12, 1973.

Maj. Gen. LEO E. BENADE,
Deputy Assistant Secretary of Defense,
Department of Defense,
Washington, D.C.

DEAR GENERAL BENADE: We had some correspondence in 1971 and 1972 concerning DOD discharge policy. In a letter to me of January 17, 1972 you stated that "In regard to your comment regarding separation designator numbers (SDN) being public knowledge, it is re-emphasized that the Department of Defense does not make SDN's a matter of public knowledge".

Recently, a news reporter requested the list defining the Separation Program Numbers, which allegedly was unavailable. It was readily supplied to him by the Army. I understand, too, that companies are able to obtain this list and use it to evaluate an applicant for a job.

I am most concerned that the information you gave me last year regarding this matter was misleading. I understood from you that this information is not available, that it is not a matter of public knowledge. Now, I know that you give it out to anyone who calls and requests it. And, that a person who has an individual's SPN number from his discharge papers can readily check this code list to see what that individual's separator designator number or separation program number signifies.

I ask you to discontinue listing these numbers on the discharge papers. The numbers serve no purpose except to make more difficult or destroy the possibilities of an individual's obtaining a job.

Sincerely,

EDWARD I. KOCH.

WASHINGTON, D.C., *March 23, 1973.*

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of March 12, 1973, regarding the availability of lists of Separation Program Numbers (SPN's).

I appreciate your feelings in this matter. The release of a partial list of SPN's to a news reporter by an individual in the Army is of concern to this office. Unfortunately, the reporter obtained the list through an Army activity which was not a user of the SPN's, nor responsible for the administration of discharge practices and procedures. Accordingly, we have taken action to reiterate the Department's policy that SPN lists will be restricted from non-governmental organizations and individuals. You may be assured that this policy will continue to be closely monitored by this office and by the Military Departments.

Notwithstanding the above, a new set of SPN's has been developed by a special joint service committee. Estimated date of publication of the new SPN's is June 1, 1973. In accordance with a Department of Defense Instruction, the list of new SPN's, including supplemental lists will be stamped "For official use only" and will be restricted from non-governmental organizations and individuals.

I trust that the information provided will be of assistance. Your continued interest in matters concerning the Military Services is appreciated.

Sincerely,

LEO E. BENADE,
Lieutenant General, USA,
Deputy Assistant Secretary of Defense.

HOUSE OF REPRESENTATIVES,
Washington, D.C., March 29, 1973.

Maj. Gen. LEO F. BENADE,
Deputy Assistant Secretary of Defense,
Department of Defense,
Washington, D.C.

DEAR GENERAL BENADE: I have your letter of March 23. The fact that the SPN code is known to those who would not otherwise be authorized makes my original comments on this matter in my letter of March 12 even more relevant. You can change that listing every month and someone will give out the information, and it will adversely affect many of the returning veterans—and for no good purpose. If you require the information for your files, why not keep it in those files? Why continue to put it on the discharge papers?

I reiterate, there is no valid reason for such action to continue. I urge you to revise the policy and to cease including the SPN listing on discharges.

Sincerely,

EDWARD I. KOCH.

WASHINGTON, *D.C., April 5, 1973.*

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in response to your letter of March 19, 1973, regarding Separation Program Numbers (SPN's).

Although it is recognized that differing views will continue to be expressed on the use of SPN's on the DD Form 214, the information on the form, including SPN's, is necessary for administrative and statutory purposes. Nevertheless, this matter has and will continue to be scrutinized to insure that our discharge policies and procedures are consistent with the Department's policy which protects against invasion of an individual's privacy. Interestingly enough, it should be noted that one reason these numbers were originally used in the early 1950's was to preserve privacy, since they were substituted for fuller, written explanations of the circumstances of an individual's discharge.

Thank you for your letter.

Sincerely,

LEO E. BENADE,
Lieutenant General, USA,
Deputy Assistant Secretary of Defense.

HOUSE OF REPRESENTATIVES,
Washington, D.C., April 12, 1973.

Hon. ELLIOT RICHARDSON,
Department of Defense,
Washington, D.C.

DEAR MR. SECRETARY: We are very concerned that the Department of Defense refuses to change its policy regarding Separation Program Numbers (SPN's). Today a letter was received from Lt. Gen. Leo Benade insisting that the use of SPN's on the DD Form 214 (discharge papers) is necessary for administrative and statutory purpose. We do not think so. Those numbers which indicate the underlying reason for the discharge allegedly, according to Lt. Gen. Benade, are restricted from "non-governmental organizations and individuals." Yet, we know, as does he, that the list of SPN numbers is easily available to reporters and indeed, we understand that one of the major American veterans organizations prints a book including SPN numbers and their classifications. What is the effect of providing these SPN numbers in this way? It is in fact to prejudice employers against certain veterans seeking jobs. To illustrate one of the most glaring situations: the same SPN number which applies to someone discharged for addiction to heroin is also used for an individual discharged for smoking marihuana. The SPN number designates one as a homosexual or alcoholic and, without question, will affect in an overwhelming prejudicial way the opportunities of those veterans to secure employment.

The Pentagon statement supports the SPN code numbers stating they are needed to determine a serviceman's eligibility for veterans benefits, his current selective service classification and his future potential for military service. That information can surely rest in the file without public revelation. Don't you agree?

We understand that this matter was called to your attention at a recent hearing by Senator Harold Hughes and that you indicated that you were unfamiliar with the matter and would look into it. We would appreciate knowing what your conclusions after an examination of the facts is.

We are introducing legislation which would ban the use of the SPN numbers on discharge documents or any other instrument available to the public. We hope, however, because the Congressional process, as you know so well, is so slow, that you will use your administrative powers to end this serious situation now. Returning veterans have other burdens to bear in securing employment and housing and re-entering civilian life. We do not think it fair to place the additional burden of SPN's on their shoulders.

We would very much appreciate your giving our request your immediate consideration and ending the practice.

Sincerely,

LES ASPIN,
EDWARD KOCH.

HOUSE OF REPRESENTATIVES,
Washington, D.C., April 23, 1973.

Hon. ELLIOT RICHARDSON,
Department of Defense,
Washington, D.C.

DEAR MR. SECRETARY: We have received your interim reply of April 18, 1973 in response to our letter regarding Separation Program Numbers.

As you know, Lieutenant General Leo Benade states in a March 23 letter to Representative Koch that a new set of SPN's has been developed by a special joint committee. The estimated date of publication of the new SPNs is June 1, 1973.

We oppose the use of any SPNs, new or old. And, having researched the matter even further, we find that there are even additional codes on discharge papers well known to those in the public interested in being aware of their meaning which have the same impact as the SPNs.

For instance, on line 11c the AR number which gives the statutory authority for the discharge appears before the SPN number. Thus, even if the SPN number were changed, one could tell from the AR number with some amount of specificity, what the reason was that the man was discharged. Even the reenlistment code number indicates a man might not be eligible to reenlist because he did not score high enough on the Army Qualification Battery.

What good is accomplished by changing one code, when there are correlated codes that can give a great deal of information about the veteran to employers who as a matter of course require to see the discharge papers. Why should anyone be able to ascertain from the discharge paper things about a veteran that he might not even know himself.

We wish to reiterate that where legitimate information exists that the military needs for its own records, it can be retained in the confidential file on that former serviceman held by the military, but that it would not be made public. There is no reason they should be used to reward or by inference punish these veterans.

We are not only now asking that the SPN numbers be removed but also these other codes which give the same information be eliminated. Does it make sense to place a former serviceman at a disadvantage with someone who was not in the military at all? That is what we are doing when we provide an employer information, sometimes adverse, to the veteran applying for a job.

These men, now veterans, certainly deserve better from us.

Sincerely,

EDWARD I. KOCH,
LES ASPIN.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., June 15, 1973.

HON. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is in further reply to your joint letters of April 12, 1973 and April 23, 1973, with Congressman Les Aspin, regarding Separation Program Numbers and other information on discharge documents.

Former Secretary Richardson has deferred any decision on this matter to Secretary-designate Schlesinger, and directed that this matter be re-studied by his staff and by the Military Services. The results of this new study should be available about July 16, 1973.

In my letter of March 23, 1973, I mentioned that a new set of SPN's was due to be published by June 1, 1973. We now expect to have these new codes approved and available to the Services by July 1, 1973. The total number of SPN's will be reduced from 530 to 126.

We will inform you as significant events occur. Your interest in matters pertaining to the Military Services is appreciated.

Sincerely,

LEO E. BENADE,
Lieutenant General, USA., Deputy Assistant Secretary of Defense.

COMMUNICATIONS RECEIVED

The unnecessary and grievous harm to an individual resulting from unfortunately common knowledge as to what the code numbers designate, and the consequent invasion of privacy which may never end for a veteran with a prejudicial SPN is graphically illustrated by the following tragic letter I received:

CONGRESSMAN EDWARD I. KOCH: Congressman Koch, I am writing to you for some help—you being a Veteran of World War two you know what the services are like and you know what discharges can do to people and there life in this sick society. I received a general discharge under honorable conditions September 25, 1958. Reason SDN–363–AFR–39–16 from the Air Force. I was told there wasn't anything wrong with it. I came from Alabama out to Sandiego California in January 1966 and went to work at R——— Corporation in Chula Vista, Calif. three weeks after Filling out Job applicant and Security Forms listing Jobs and type of discharges received my name has been drug thru Slimmy Filth by Foreman and worker and even to Where I live and When I go to town I am treated like I have the Plague. I have been to the Veteran Administration and asked them What Is Wrong With a General discharge Under Honorable Conditions and What a AFR–39–16 Reason SDN–363 mean't they said they did not know and that I should get the Red Cross are a lawyer to help me that they couldn't. I Went to the District Attorney In Chula Vista and asked what I could do about being Slandered and If I could see R——— Corporation Security File own me.

He said unless I could get a Witness to Swear he heard me being slandered that I had best forget It and that R——— Corporation could have a Security File own me. I asked What Would happen if I beat Hell out of them he said I could get 6 months to ten year. Plus being Sued by them.

I know we are living in a sick society with all the corruption all for a dollar that is worth 21 cents. Congressman Koch the only thing I am guilty of is letting boredom and disgust and bad food and whiskey break me after 14 months of 18 month tour in England where while drunk and depressed I tried to commit suicide and if anyone says different they are a dam liar. What I need is a complete copy of everything in my Air Force files including my medical records to clear my name if there is any justice in this country. If you can help me I would appreciate it. My old Air Force number was AF Rank A2/C C.M.G. Congressman Koch you are my last hope of getting help and justice.

Thank you.

———, ———.

U.S. HOUSE OF REPRESENTATIVES,
Washington, D.C., June 28, 1973.

Lt. Gen. LEO E. BENADE,
Deputy Assistant Secretary of Defense,
Department of Defense,
Washington, D.C.

DEAR GENERAL BENADE: You have indicated in your previous letters a belief that the use of SPN's on discharge certificates was for "administrative and statutory purposes" only, and that such inclusion does not offset the privasion of privacy for the veteran.

I include for your edification a photocopy of the latest in a series of communications from citizens who are considerably aggrieved by the rank injustice the inclusion of SPN's have caused. The present case being submitted is especially sad, and holds the potential for real tragedy, as I think you will agree. However, for every complaint received, there are surely thousands of people who are suffering silently as a result of Defense Department policy.

I reiterate my point made in earlier communications and not fully spoken to by you; not only the codes and designations of the SPN's be kept confidential, they should not be entered on the discharge certificate at all.

I would very much appreciate it if you could have the submitted case investigated and communicate to me its disposition.

Sincerely,

EDWARD I. KOCH.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, D.C., July 6, 1973.

HOWARD H. CALLAWAY,
Secretary of the Army, Department of the Army, The Pentagon, Washington, D.C.

DEAR MR. SECRETARY: May I congratulate you on your new appointment and confirmation as Secretary of the Army. In your thoughtful letter of May 19, 1973 you mentioned the welcoming of suggestions as to how to make the Army better.

As you may be aware, I have been engaged in trying to have Separation Discharge Numbers deleted from the discharge papers of all veterans, past and present, as well as forbidding the dissemination of the SPN designation to any private person or entity. At present, the widespread knowledge of these designations especially by employers, constitutes an invasion of privacy, as well as being tantamount to a denial of due process.

I am seeking both through administrative and legislative means to rectify this totally unfair practice. I urge you to make a recommendation to Secretary Schlesinger against the continuation of this policy.

In addition, would you kindly send the list of new Separation Program Numbers and the study on this issue that is scheduled to be made available about July 16,

1973 according to the enclosed letter of General Benade, Deputy Assistant Secretary of Defense for Military Manpower Policy.

I wish you success in your new post and hope that we may have an open and friendly working relationship.

Sincerely,

EDWARD I. KOCH.

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., July 18, 1973.

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This is an additional interim reply to your joint letters of April 12, 1973, and April 23, 1973, with Congressman Les Aspin, regarding Separation Program Numbers (SPN's) and other information on discharge documents.

First, our review of Separation Program Numbers and Reenlistment Codes has not been completed. You can be assured that any decisions resulting from this review will be sent to you as soon as possible.

Second, the Standardization of Data Elements and Codes has been approved. While it has been approved for publication within the Services, implementation and use by the Services will not be earlier than July 1, 1974. Even this projected date may not be firm for all of the Services. The essence of this standardization is the adaptation of 126 SPN's from 530 previous SPN's of all of the Services.

We will continue to keep you informed.

Sincerely,

LEO E. BENADE,
Lieutenant General, USA, Deputy Assistant Secretary of Defense.

JULY 31, 1973.

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: The Secretary of the Army has asked me to reply to your letter concerning the Separation Program Designators.

Your continuing interest in the preservation of individual privacy is appreciated and the Army shares this concern. As you are aware, the recording of Separation Program Designators is the mechanism by which the military departments certify to other interested Government agencies the nature of a veteran's service. By this procedure, the Executive branch implements the statutes providing veterans preferences for a wide range of benefits. It also serves important statistical purposes in our continuing attempt to improve our personnel management practices. Thus, the objective of our recommendations to the Department of Defense has been to attempt to strike a balance between these governmental needs and the individual's right to privacy.

As an initial action, you may be interested in knowing that we have designated our current listing of Separation Program Numbers as "For Official Use Only." This was done to assist in restricting knowledge of the specific basis for separation to the government agencies that may need this information. While the final position has not been determined by the Department of Defense, we understand that a new regulation listing Separation Program Designators will also be "For Official Use Only" and will be a joint service publication for which the Department of Navy has primary proponency. The new regulation has not yet been published, but when it is, you will be provided a copy.

You may be assured that this area has our continuing interest and your comments and thoughts are appreciated.

Sincerely,

JOHN L. NALER,
Chief, Investigations and Legislative Division.

HOUSE OF REPRESENTATIVES,
Washington, D.C., September 7, 1973.

JOHN L. NALER,
Chief, Investigations and Legislative Division, Department of the Army, Washington, D.C.

DEAR MR. NALER: I have your letter with regard to SPN numbers. So what's new? You continue to defend the use of the SPN designators and the defense is based on the fact they are to be used "For Official Use Only" when you know, or at least should know, that the code becomes available to private employers. I have already stated to you that whatever information you believe to be appropriate for your files in order to provide the interested government agencies with information they need regarding the nature of a veteran's service can be maintained in a confidential file, and does not require that it be placed on the veteran's discharge paper for all to see.

If only you would read some of the letters I have received from individuals who have suffered as a result of the divulgence on their SPN numbers to unauthorized persons and the consequent embarrassment to them, even you would change your mind.

Sincerely,

EDWARD I. KOCH,

ASSISTANT SECRETARY OF DEFENSE,
Washington, D.C., November 16, 1974.

Hon. EDWARD I. KOCH,
House of Representatives,
Washington, D.C.

DEAR MR. KOCH: This letter is in further reply to your inquiry regarding Separation Program Numbers (SPN's).

During his confirmation hearings before the Senate Armed Services Committee on June 18, 1973, Mr. Schlesinger deferred a final judgment on the subject of SPN's until a second Department of Defense study was completed. We have just completed this thorough review, and we have again concluded that there is no total solution which will balance the competing interests of safeguarding the rights of those who served honorably and received a favorable discharge, and, at the same time, preventing or minimizing stigmatization of those who receive adverse discharges or codes.

Critics have alleged that SPN's unduly stigmatize veterans who are discharged with honorable discharges but for adverse reasons. In such cases, the nature of their service is categorized as honorable, but the individual's potential for future service is limited by the reason for discharge (e.g., inaptitude). These ex-service members are normally released prior to completing their tour enlistment. Representing this view, several bills which would delete any coding of the reason for discharge from discharge certificates have been introduced in both Houses of Congress.

As a result of the previous August 1972 study, no changes were made in the basic SPN policy, although the Secretary of Defense directed that three related actions be taken:

1. SPN's were made "For Official Use Only."

2. A small number of SPN's had been supplemented by narrative explanations. These narrative explanations were removed.

3. SPN's were examined to determine whether additional SPN's were needed in order to allow more differentiation of the reasons for discharge, especially in the areas of drug and alcohol abuse. The drug abuse discharge authority was identified as requiring more differentiation to provide for administrative discharge on the basis of unsuitability or unfitness. This change is in the final stages of coordination.

In addition, we have standardized the 530 SPN's of the Military Services to 126 common identifiers. These will be implemented on July 1, 1974, at the beginning of the next Fiscal Year.

The most recently completed study considered a wide range of alternatives to our present policy. We concluded that in no case would a change effectively remove the stigmatization of the relatively few who are adversely discharged without significantly depriving the vast majority of veterans who are favorably discharged of their right to a military document which would provide ready assistance to

veterans' benefits, civilian employment or reenlistment. For instance, if SPN's were deleted from separation documents:

1. Those adversely discharged would gain little because the reason for discharge is fact and is documented in the personnel record. The Freedom of Information Act requires that upon application of the veteran, such information must be released to him. Thus, any employer may continue to require documentation from the individual of the reason for his discharge.

2. Those favorably discharged would not have ready access to Veterans Administration benefits nor to a readily available employment reference to assist them in their transition to civilian life. Once the individual realized that this information would be of value to him he would have to apply to the Services or to the National Personnel Records Center for the information. As noted above, the Freedom of Information Act requires that the information be released to the individual. Therefore, no gain would be made over the present system.

Even if SPN or reenlistment coding were deleted from the Department of Defense Form 214, "Report of Separation From Active Duty," other personnel information on the form could contain adverse implications. For instance, low rank at discharge, AWOL or confinement time, total length of service less than full enlistment, or the lack of a good conduct medal—all provide clues to the reader who is knowledgeable of military service.

We thus reaffirmed our position in favor of the veteran who serves honorably and who is discharged under favorable circumstances. The DoD Form 214, the summary of pertinent personnel information including SPN's and reenlistment codes, is necessary to protect his equity in the quality of his military service.

Enclosed is a fact sheet that discusses this subject in more detail.

As a matter of information, an identical letter has been forwarded to Chairman John C. Stennis of the Senate Armed Services Committee and F. Edward Hébert of the House Armed Services Committee, to Senator Hughes and Symington, and to Congressman Aspin, Conyers, and Drinan, in response to their previous inquiries.

I trust that this information will be of assistance to you. Your interest in matters pertaining to the military services is appreciated.

Sincerely,

LEO E. BENADE,
Lieutenant General, U.S. Army, Deputy Assistant Secretary of Defense.

FACT SHEET: USE OF SEPARATION PROGRAM NUMBERS (SPN'S) ON DD FORM 214

I. BACKGROUND INFORMATION: TYPES OF DISCHARGES

There are three types of administrative discharges—honorable, general or undesirable—and there are eleven general grounds upon which a member may be administratively discharged from the Armed Forces:

1. Expiration of Enlistment
2. Convenience of the Government
3. Resignation—Own Convenience
4. Dependency or Hardship
5. Minority
6. Disability
7. Unsuitability
8. Security.
9. Unfitness
10. Misconduct
11. Resignation in lieu of court-martial

An honorable or general discharge may be issued to an individual who is separated for any of the eleven reasons. An undesirable discharge may be issued only if an individual is separated for one of the last four listed grounds. Even in these cases, however, the individual may receive an honorable or general discharge; the issuance of an undesirable discharge is permissive, not mandatory.

In addition to administrative discharges, punitive discharges (bad conduct and dishonorable) are issued only as a result of sentence by court-martial.

Honorable and general discharges are considered under honorable conditions; undesirable, bad conduct dishonorable discharges are under less than honorable conditions.

II. SEPARATION PROGRAM NUMBERS ON DD FORM 214

When an individual is separated from a Military Service, he is furnished:

A discharge certificate: honorable, general, undesirable, bad conduct, or dishonorable.

A DD Form 214, "Report of Separation From Active Duty." (formerly entitled, "Armed Forces of the United States Report of Transfer or Discharge")

SPN's are data processing identifiers of reasons for discharge. An individual's SPN is placed on the DD Form 214 in conjunction with the regulatory authority for the discharge or separation from military service, SPN's are not placed on the discharged certificate.

The DD Form 214 is a concise source document, completed by the Services and used by them and other government agencies. Copies are furnished to the Veterans Administration (VA) and the Selective Service System (SSS). It is of value to the individual as immediately available documentation of his military service and often serves as an employment reference.

There are approximately 35 categories of personnel information on the DD Form 214 which the Services use for statistical reporting, research and sampling. Although the Services are its prime users, the decision to add, delete, or change parts of the form during the last 20 years has been jointly made by its governmental users. These decisions have been guided by the desire to improve the form and to increase the capability to make certain determinations, such as the former serviceman's potential for future military service; his eligibility for veterans' benefits; and his current Selective Service classification. At a minimum, 20 of the 35 categories of information on the form are necessary in varying degrees to make these determinations. The SPN is one of these data elements.

There is a SPN for each reason for separation. Examples of separations other than discharges are retirement, dismissal, release from active military service, and separation to continue active duty in another status. The information for the individual's DD Form 214 is extracted from the individual's personnel record. It is possible to receive an honorable or general discharge (both are under honorable conditions) and receive a SPN which is considered adverse. Examples of this situation are when the SPN reflects drug abuse, failure to pay debts, or homosexuality. The specific nature of service may have been honorable but the potential for future service is limited by the reason for discharge.

The original copy of the DD Form 214 is given to the individual. The Department of Defense does not provide information to employers. Information from personnel records is released only to the individual, his authorized agent, and governmental agencies who have a legitimate need for the information. As a practical matter, employers may demand that an individual present his DD Form 214 as a condition of employment.

The need for the SPN on the individual's copy of the DD Form 214 can best be illustrated by its use by one of the document's secondary users, the Veterans Administration. Physical disability is a reason for discharge. There are approximately 20 different reasons for a physical disability discharge, some of which might be considered to have an adverse connotation. In order for the Veterans Administration to advise former servicemen promptly and accurately of their eligibility for benefits under various Public Laws (disability compensation, vocational rehabilitation, in/out patient medical treatment, disability pension), the VA uses the physical disability reason shown on the individual's copy of the document. Such prompt determination is of extreme importance to disabled former servicemen.

In addition, the vast majority of our veterans benefit by having a prior employment reference readily available for presentation to prospective employers. Even if the SPN were deleted from the DD Form 214, no practical gain would be made. Many prospective employers would continue to require prior employment references and either would not hire the veteran or would hire him conditionally, until he obtained the information. The individual would have to request the information from the Services or the National Personnel Records Center, and the Freedom of Information Act requires that this information be provided to him. The decision to provide this information to the prospective employer would still, as exists today, remain with the individual. The end result could well be a decision by prospective employers to avoid hiring recently discharged veterans because they lack timely and complete prior employment references.

If DoD no longer provides the individual with a document usable as an employment reference and if he later requests information, we would be tasked to

research and provide the information to him from his personnel files as required by the law. Our present system of issuing the DD Form 214 saves considerable workload and expenses in answering personnel inquiries. In addition, present procedures require the serviceman to review and sign the DD Form 214 at the time of separation. This procedure validates the accuracy of the information on the form and forecloses claims that the serviceman did not know the reason for his discharge.

III. RECENT REVIEWS OF SPN POLICY

A study of SPN policy was completed in August 1972 which reviewed the practices and procedures relating to the use of SPN's on the separation document for consistency with Department of Defense policy which protects against the invasion of privacy of the individual. These practices and procedures were analyzed in detail and it was determined that they were necessary for legitimate administrative and statutory purposes, and were consistent with the policy against invasion of privacy. However, three actions were directed:

1. Master lists of SPN's would be marked "For Official Use Only" and their use limited to Governmental agencies.
2. No narratives would be used in conjunction with SPN's. This would afford the individual additional protection from possible stigmatization which could result from words being used to describe the reason for discharge.
3. An examination of SPN's would be made to see if additional SPN's were needed to permit greater differentiation in the reasons for discharge.

These actions have been completed. New SPN's were developed to provide greater differentiation of drug and alcohol abuse. In addition, the 530 SPN's of all the Services were standardized to 126 joint SPN's. These new SPN's should be implemented on July 1, 1974, as the beginning of the next Fiscal Year.

A second review of SPN policy was completed in October 1973. This study considered a wide range of alternatives to our present policy. We concluded that in no case would a change effectively remove the stigmatization of the relatively few who are adversely discharged without significantly depriving the vast majority of veterans who are favorably discharged of their right to a military document which would provide ready assistance to veterans' benefits, civilian employment or reenlistment.

DoD thus reaffirmed its position in favor of the veteran who serves honorably and who is discharged under favorable circumstances. The DoD Form 214, the summary of pertinent personnel information including SPN's and reenlistment codes, is necessary to protect his equity in the quality of his military service.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, D.C., February 13, 1974.

Lt. Gen. LEO E. BENADE,
Deputy Assistant Secretary of Defense, Department of Defense, Washington, D.C.

DEAR GENERAL BENADE: I am still concerned with the problem of SPNs and the refusal of the Pentagon to change its policy in this matter. The policy I refer to of course is set forth in your letter of November 16, 1972.

In that letter you refer to two studies conducted by the Department of Defense, one completed in August '72 and the other in October '73. I would appreciate your providing me with copies of these two studies.

I would appreciate your expenditing this request.

Sincerely,

EDWARD I. KOCH.

MARCH 21, 1974.

DIRECTOR,
Correspondence and Directives Division, OASD(A), The Pentagon, Washington, D.C.

DEAR SIR: This letter written on behalf of Congressman Edward I. Koch, is a formal request pursuant to the Freedom of Information Act, 5 U.S.C. § 552, for access to two Defense Department studies pertaining to the use of Separation Program Numbers (SPN's). These studies, one in August 1972 and the other in October 1973, are referred to in a letter from Lieutenant General Leo E. Benade,

Deputy Assistant Secretary of Defense, to Congressman Koch on 16 November 1973. (A copy of that letter is enclosed for your convenience). Congressman Koch requested these studies on February 13, 1974, which request was denied in a letter from Lieutenant General Benade on March 12, 1974.

If we do not receive a substantive response to this letter within 10 days, we will consider the request denied.

Very truly yours,

RAYMOND T. BONNER.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, D.C., March 27, 1974.

Secretary JAMES R. SCHLESINGER,
Department of Defense,
Washington, D.C.

DEAR MR. SECRETARY: Your recent action in authorizing the removal of Separation Program Numbers and reenlistment code numbers from all discharge papers deserves congratulations and support. It is a decision which, as you know, has been urged for a long time by many Members of Congress.

However, I feel that it is not enough to merely let the veteran request a new discharge certificate. A great part of the problem has to do with the fact that veterans do not know that the SPNs exist on their discharge papers. Their employers might know it—but they do not. Consequently, it is difficult to imagine that any substantial percentage of veterans would be aware they can request new papers.

It is the responsibility of the Department of Defense to guarantee that the rights to privacy of veterans is assured. To do this I believe that the DoD should send to all those veterans discharged since the early 1950s, when SPNs were instituted, updated DD Forms 214—superceding the discharge paper issued when they were discharged from the service—which would not show these SPNs or reenlistment code numbers.

I also believe that there can be coercion on the part of employers who request that veterans authorize the release of SPNs to them. I propose that the information not be supplied to an employer or third parties, even with the veteran's consent, so as to protect the veteran against pressure.

I urge your immediate consideration of these provisions in developing your regulations on this issue and I would appreciate your advising me of your position as soon as possible.

Sincerely,

EDWARD I. KOCH.

Mr. GOLDWATER. I thank the gentleman from New York (Mr. Koch) for his contribution. I certainly recognize him as one who has been greatly concerned in this area of privacy.

I should like to recognize at this time, the gentleman from New York (Mr. Horton) one of our sponsors on the special order.

(Mr. HORTON asked and was given permission to revise and extend his remarks.)

Mr. HORTON. Mr. Speaker, I thank the gentleman from California for yielding this time to me. I want to commend him and Mr. Koch for their initiative on this special order.

Mr. Speaker, I am proud to serve as a sponsor of this special order to emphasize the congressional commitment to privacy. The six sponsors of this discussion represent both parties and a broad spectrum of political view points. We are united, however, by mutual concern for threats to individual privacy and by our hope that the Congress will even more vigorously pursue efforts to safeguard the individual in our society.

The climate has never been more propitious for congressional action. That is so because the administration has joined the call for privacy initiatives. The President said in his state of the Union address:

"One measure of a truly free society is the vigor with which it protects the liberties of its individual citizens. As technology has advanced in America, it has increasingly encouraged on one of those liberties that I term the right of personal privacy. Modern information systems, data banks, credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another—all these have left millions of Americans deeply con-

cerned about the privacy they cherish. The time has come, therefore, for a major initiative to define the nature and extent of the basic rights of privacy and to erect new safeguards to insure that those rights are respected..

"I shall launch such an effort this year at the highest levels of the administration, and I look forward again to working with this Congress in establishing a new set of standards that respects the legitimate needs of society and that also recognizes personal privacy as a cardinal principle of American liberty."

Consistent with this statement, the President has created in the White House a Domestic Council Committee on the Right of Privacy. It is chaired by Vice President Ford and includes several highranking administration officials. This committee is directed to examine four areas of concern:

Federal Government methods of collecting information on people and of protecting that information;

Procedures which would permit citizens to inspect and correct information held by public and private organizations;

Regulations of the use and dissemination of mailing lists; and

Ways that we can safeguard personal information against improper alteration or disclosure.

I am pleased to note that the one suggestion which the Domestic Council Privacy Committee has already made has been accepted by the President: in accordance with a recommendation approved unanimously by the House Government Operations Committee, an Executive order granting the Agriculture Department access to the tax returns of over 3 million American farmers has been revoked.

I welcome the President's initiative in the area of privacy, and I welcome his action in invalidating an ill-conceived Executive order. I hope that these acts are indicative of a genuine effort to be of assistance to those of us who have been attempting for many years to preserve citizens' rights to privacy.

Mr. Speaker, I am privileged to serve as ranking minority member of the Committee on Government Operations, which has demonstrated a strong interest in protecting citizens' rights to privacy over the past decade. Its Special Subcommittee on Invasion of Privacy, of which I was a member, was established in 1964. This panel performed highly useful investigations in such areas as electronic surveillance, data banks, mail covers, and psychological testing.

For the last several years, the Government Operations Committee's concern for privacy rights has been manifested primarily through the Foreign Operations and Government Information Subcommittee, of which I have also been a member. That subcommittee, ably chaired by our colleague from Pennsylvania, Mr. Moorhead, has held important hearings on privacy implications of advanced information technology, Government use of polygraphs, and use of private information by Government employees.

The Foreign Operations and Government Information Subcommittee is currently considering a bill by the gentleman from New York (Mr. Koch) to grant individuals access to records about them maintained by Government agencies. I am hopeful that constructive legislation based on the concepts of this measure will be forthcoming.

Mr. Speaker, I would like to draw attention to another bill which is now pending before the Foreign Operations and Government Information Subcommittee—a bill which I have sponsored for several years to protect individuals whose privacy is threatened because their names and addresses appear on Federal mailing lists.

In 1970, Wendell Ames, an eminent doctor in my congressional district, reported to me that he received solicitations from a firearms merchant shortly after registering as a gun collector with the Alcohol, Tobacco, and Firearms Division of the Internal Revenue Service. The firearms company was using what appeared to be duplicates of the IRS mailing label. Inquiries revealed that the IRS was selling lists of individuals who had registered as collectors of guns at a cost of less than one-tenth of 1 cent per name. The dangers inherent in this practice are obvious. Fortunately, I can report that following my inquiries, the IRS agreed to cease the sale of lists of gun collectors, but they persisted in making lists of gun dealers available.

Surveys of Federal agencies have revealed that there is no pattern, no rhyme nor reason to Federal agency policy on the subject of mailing lists. Some agencies make lists available on a regular basis—citing the Freedom of Information Act as authority. Others deny access to all such lists—again citing the Freedom of Information Act. In fact, the policy of the Federal Government is no policy at all.

My bill, H.R. 3995, would clarify this situation by setting a reasonable govern-

mentwide policy which protects individual privacy while adequately safeguarding the public's right to know. H.R. 3995 is limited to prohibiting a Federal agency from distributing lists of names and addresses of individuals—either employees or those having business with an agency, where such lists are to be used for commercial purposes or other solicitation or for purposes prohibited by law.

Mr. Speaker, I urge my colleagues to examine the hearing record on my bill as it will demonstrate the tremendous potential abuse that can result without a clear Government policy on the availability of literally thousands of Government-held lists. More than 60 of my colleagues have joined me as a sponsor of the bill and I hope that others will lend their support to this proposal.

Mr. Speaker, the participants in this special order will set forth an impressive record of congressional initiative in the privacy area. I have described briefly the important work that has been ongoing in our Government Operations Committee and I know that my colleague, Mr. Moorhead, will expand on the contributions his subcommittee has made. Equally impressive is the work of the Judiciary Committee, particularly related to criminal justice records. But despite the progress we are making, I remain convinced that the Congress is not now equipped to deal with privacy issues on the level those issues demand.

For that reason, I have sponsored legislation for many years to create a Select Committee on Privacy to give breadth and forward thinking to assaults on individual privacy.

The House, traditionally the democratic institution closest to the people, has the obligation and duty to inform itself fully about the range of threats to individual privacy. Because of the immense power of the new technologies of data collection and processing, behavior control, and communication, all of which affect privacy and other individual rights, we need our own source of expertise if we are to legislate in the best interests of the Nation. The select committee could provide that source and would be equipped to understand and evaluate the long-term effects so often overlooked in our rush to deal with immediate problems. Its fundamental task would be to give visibility to ideas now buried within the Federal bureaucracy, in private business, or in academic circles before they erode the integrity of the individual citizen or dictate future American lifestyles. I am confident that our discussions today will demonstrate the need for this type of forum in the House.

Mr. GOLDWATER. I thank the gentleman from New York for his contribution and certainly also recognize the contribution the administration has given by its indication of action currently in appointing the Vice President to head this Commission.

Mr. Speaker, I yield now to the gentleman from Arkansas (Mr. Alexander).

(Mr. ALEXANDER asked and was given permission to revise and extend his remarks and include extraneous matter.)

Mr. ALEXANDER. Mr. Speaker, I am pleased to join my colleagues in this effort to focus attention on one of our most precious rights as citizens of these United States—the right to privacy.

The American experiment in democracy rests on the belief that Government meddling in matters of individual concern is an evil, as Jefferson said, "no less obnoxious when it is essential." While the Constitution confers no absolute right to be let alone, it does limit the scope of permissible Government intrusion and demands a special sensitivity to the right of privacy in those areas in which it is not strictly prohibited. The Founding Fathers knew that a free government must consciously limit itself in order to safeguard "the right of the people to be secure in their persons, houses, papers, and effects."

We are faced with a threat to that right. One of our own making over which we exercise at present only minimal control. That threat is the unprecedented capacity and need by government at all levels to digest information. The capacity of the bureaucracy to handle mountains of often personal data is of course the product of computer technology. The need to do so derives from the increasing demand on our governmental institutions to organize, plan, in short govern, a complex society. But as Jefferson observed, this need makes the practice no less obnoxious and so we must be alert to the ever present possibility of abuse.

For this reason, I and a number of my colleagues were disturbed by the publication of Executive Orders 11697 and 11709 which granted authority to the Department of Agriculture to inspect the personal tax returns of 3 million American farmers. This authority was as comprehensive as it was unprecedented. Apparently any employee of USDA could be authorized by the Secretary to inspect the tax return of any farmer. The House Subcommittee on Foreign

Operations and Government Information of the Committee on Government Operations, on which I serve, learned in testimony from the Office of the Attorney General and the Department of the Treasury, that these orders were prepared as a prototype for future tax return inspection orders.

As I stated on February 19, 1974:

"These executive orders present the frightening prospect that the administration is attempting to begin the process of making personal income information of whole classes of people available to various departments and agencies without regard to the private nature of the information, or protecting individuals from possible abuse."

Such a development would hardly be a proper safeguard for that right of privacy described by the President as a "cardinal principle of American liberty."

I am pleased to note that after concentrated and sustained pressure from the Congress, the public, a perceptive member of the press—Alan Emory, of Watertown, N.Y., Daily Times—and the IRS itself, this improvident grant of authority has been rescinded by Executive Order 11732 on March 24, 1974.

Unfortunately, the chilling specter raised by these orders continues. I am alarmed by the technical capacity of government to retrieve from its computer banks a dossier on individuals combining bits and pieces of data gleaned from many sources. The collection of such information is easily justified as enhancing administrative convenience and efficiency; it is just as easily subverted into a genuine, sinister force. An enlightened public should not quickly forget the articulated desire of an ex-White House official, John Ehrlichman, to make the Internal Revenue Service "more politically responsive."

Potential political operatives zero in on IRS files for the same reason that the Congress must now step in to assure their integrity and continued confidentiality; an individual's tax return contains a wealth of information about his private affairs, his job, his income, his charitable interests, his family responsibilities. The accurate reporting of all of these matters is indispensable to the administration of our Federal tax system. The remarkable candor shown by the American people each April 15 should not be taken for granted. Congress must take immediate steps to guarantee that the information so gathered is not used for any other purpose not specifically authorized by law.

Any statistical data needed by the administrative arm of the Government should be collected by the Bureau of the Census, the body established by the Congress for that purpose. It is interesting to speculate on why, if USDA believed this type of information was vital to its operations, it eliminated from its 1974 budget all funds for a farm census. Administrative efficiency is a goal to be sought in Government. But the possibility of individual tax returns becoming the bedtime reading of politicians or bureaucrats is simply too high a price to pay for it.

I do not presume that such was the intention of those in the executive branch who supported this relaxation of the confidentiality of IRS files. But the classic atmosphere of personal privacy is a political climate in which each person decides for himself what personal information he will share and with whom he will share it. And as Mr. Justice Brandeis said:

"The greatest dangers to liberty lie in insidious encroachment by men of zeal, well meaning but without understanding."

I wish to make a part of the Record several news stories on this controversy written by Alan Emory of the Watertown, N.Y., Daily Times:

[The articles follow:]

[From the Watertown (N.Y.) Daily Times, Oct. 29, 1973]

FARM TAX SNOOPING SCRAPPED

(By Alan Emory)

WASHINGTON.—The Agriculture Department has decided temporarily, in the face of a hostile reaction from Congress, farmers and civil liberties groups, to shelve President Nixon's order allowing it to inspect individual tax return of farmers.

Assistant Attorney Gen. Robert G. Dixon, Jr., had said the order was drawn up as a model so that tax returns could be used for statistical purposes by other federal agencies. He insisted there was no intent to invade farmers' privacy because the department wanted only "group data" and not data on individual farmers "which would certainly be a matter of great concern."

CONCERNED

"Mr. Dixon should have been greatly concerned," a House Government Operations sub-committee reported, "because that is precisely what the Department of Agriculture was authorized to get."

The Statistical Reporting Service in the department had felt that, despite steadily refined programs of reporting by farmers, still greater precision was necessary. It obtained from President Nixon an executive order—in broad language in January and modified in March—allowing the Agriculture Department to obtain names, addresses and gross income or product sales of farmers from Internal Revenue Service records.

Ironically, the IRS itself had strongly opposed providing personal information from tax returns.

Although the Nixon order affected 3,000,000 farmers, no public or press announcement was made by the White House or the Agriculture Department. The order and regulations were published in the Federal Register, which, one farm spokesman said, was "not every-day reading for the average farm family." No farm leaders were consulted.

DATA VITAL?

Rep. Bill Alexander, D., Ark., said if the data were vital to Agriculture Department operations, as claimed, then President Nixon would not have wiped out farm census funds from his fiscal 1974 budget.

Several congressmen and IRS officials favor giving the Agriculture Department names and addresses of farmers and letting the department ask the farmers for the financial information sought.

"No one asked a single farmer whether he was willing to share this personal financial information with the department," Alexander said.

He asked whether the order would prove a model for the Commerce Department to inspect tax returns of businessmen, the Housing and Urban Development Department to examine returns of homeowners receiving government-insured loans, the Labor Department to look at wage earners' returns or the Health, Education and Welfare Department to pry into returns of doctors and teachers.

Dixon said the Justice Department was not requested to express "any policy judgment," and it did not. Alexander called this a "blatant disregard for the rights of private citizens."

HEALTH PLANS

J. Richard Grant, an official of the Statistical Reporting Service, said that the opposition had halted any department plans to pursue access to farmers' data with the IRS "directly."

In an interview, he said that the department had no access to "individual names and addresses" through census data and deplored the "misinformation" about department need for the details and what would be done with them.

Donald O. Virdin, former IRS disclosure staff chief, told the House panel, headed by Rep. William S. Moorhead, D., Pa., that it would be "no problem" to provide the Agriculture Department quickly with names and addresses of the 3,000,000 farmers "if that is all Agriculture wants."

The committee said most farmers would probably be glad to furnish the information if they knew how it would help them and they were assured it would be kept confidential and used just for statistical purposes.

The Justice Department had said that the original, broadly-worded Nixon order that was later changed, "was prepared by the Department of the Treasury—as a prototype for future tax return inspection orders."

Alexander called that a "frightening prospect that the administration is attempting to begin the process of making personal income information of whole classes of people available to various departments and agencies without regard to the private nature of the information."

The House Government Operations Committee recommended that the IRS give the Agriculture Department only names, addresses and taxpayer identification numbers and no personal financial data unless the individual voluntarily consented in writing after an Agriculture Department request.

Several congressmen are drafting legislation making tax returns explicity confidential, with the only loophole approved by Congress.

[From the Watertown (N.Y.) Daily Times, Feb. 26, 1974]

ISSUE OF FARM INCOME TAX INSPECTION TO BE TURNED OVER TO NEW COMMISSION

(By Alan Emory)

WASHINGTON.—President Nixon says the issue of his controversial executive order allowing the Agriculture Department to inspect key features of individual farmers income tax returns will be turned over to a new federal commission on privacy headed by Vice President Ford.

The President was asked at his Monday night news conference how he explained the executive order—and a Justice Department opinion saying it should serve as a "a model" for all executive departments—in the light of his strong defense of confidentiality for White House papers and his new protection-of-privacy policy for individual citizens.

Nixon conceded that he had not specifically raised the question of tax returns in his privacy message Saturday, but he wanted it considered, along with credit bureau computerized files on individuals.

Not only business concerns, but the federal government itself has taken action that could "impinge" on privacy, Nixon admitted.

The President said the whole question should be considered by his new commission.

Nixon, however, did not offer to withdraw the order which has drawn sharp criticism among farm groups and in Congress, nor did he comment on the Justice Department opinion, which many observers believe opens the door for widespread abuse of income tax return confidentiality by a host of federal agencies.

The Internal Revenue Service had objected to the Nixon order, issued early in 1973 and then slightly modified.

[From the Watertown (N.Y.) Daily Times, Feb. 28, 1974]

IRS IGNORES NIXON ORDER ON FARMERS TAX RETURNS

(By Alan Emory)

WASHINGTON.—The Internal Revenue Service has indicated privately it will not enforce President Nixon's executive order authorizing Agriculture Department examination of key parts of farmers' individual income tax returns.

However, Agriculture Secretary Earl L. Butz has twice refused congressional requests to shelve the order.

President Nixon said Monday night that the wisdom of the order—which the Justice and Treasury Departments say will serve as a "model" for other federal agencies—would be studied by a new commission headed by Vice President Ford.

Rep. Jerry Litton, D., Mo., who uncovered the order, held hearings on it and is sponsoring legislation to tighten IRS rules about allowing others to see tax turns, said the measure had a "good chance" in the House Ways and Means Committee.

He said the IRS was supporting the legislation, but unofficially, since it conflicted with the executive order.

Litton said, in an interview, Nixon's move amounted to authorizing the Vice President to determine whether action Nixon himself had taken was "proper."

The Congressman said that was "strange," since the President had not given Ford much authority in any other field.

When Litton originally introduced legislation to kill the Nixon order, but permit the Agriculture Department to obtain just farmers' names and addresses, the department cold-shouldered the idea and would not even comment on it.

After Litton sponsored his measure to tighten the IRS rules about who could see tax returns, however, the department indicated an interest in the first bill.

Litton said he had been surprised when listening to President Nixon's State of the Union message, to hear "a man who proposed opening up 3,000,000 tax returns talking about privacy."

Litton said the Agriculture Department had been asked if it placed so much importance on getting facts that it needed tax return details, and officials said it did.

If that were true, he then asked them, why were funds for an agricultural census struck from the budget.

"I have yet to get an answer," he told a reporter. "The census form goes to every farmer. A tax return sampling would not be as complete. Either they need the information or they don't."

According to Litton, the first request for the order on tax returns went to George P. Shultz, then director of the Office of Management and Budget, but nothing happened. Three years later the order was drafted at the Treasury Department, where Shultz was secretary.

"Why wait three years and then give the Agriculture Department broader authority than it asked for?" Litton asked. "The department did not want to look at the tax returns, but the executive order not only authorized it to, it spelled out how the department should do it."

Litton recalled that former Nixon aide, John D. Ehrlichman, had promoted a policy of making the IRS "more politically responsive" and theorized that the administration wanted the order on farmers' returns because "if they could get away with that they could try another field later."

The Congressman said the House Government Operations Committee, as well as one of its subcommittees, had asked Butz to hold up on implementing the executive order and that he refused.

[From the Watertown (N.Y.) Daily Times, Mar. 1, 1974]

IRS Still Opposes Scrutiny of Returns

(By Alan Emory)

Washington.—The split within the Nixon Administration over opening up individual income tax returns is coming closer to the surface.

Internal Revenue Commissioner Donald C. Alexander, plainly uncomfortable over an executive order by President Nixon designed to allow all federal agencies a shot at individual returns says he is insisting his agency "guard the taxpayer's right of privacy."

The Nixon order, issued last year without a public hearing or any notice is drawing increasing fire in Congress, from farm groups—since it applies to Agriculture Department inspection of individual farmers' returns—and civil liberties organizations.

Rep. Bill Alexander, D-Ark.—no relation to the commissioner—one of the first to uncover the order and ask for Congressional action—calls it a "massive invasion of the rights of privacy of an entire class of Americans" and "an extremely dangerous precedent to all other groups of citizens of whatever occupation."

Despite the Nixon order Commissioner Alexander revealed in a letter to Rep. William S. Moorhead, D-Pa., his agency is limiting "a mailing list of names and addresses of farmers."

Alexander said he supported legislation to make tax returns "explicitly confidential" except for tax administration and enforcement—a House Government Operations subcommittee on foreign operations and government information.

Moorhead is the sub-committee chairman.

Alexander says tax returns should be "confidential and private" unless Congress "clearly specifies" to the contrary.

He said the IRS was barring tax returns to outsiders except where there are "sound reasons" for their availability, and it was "consistently applying such a disclosure philosophy" while working toward a goal of "ensuring the confidentiality of federal tax return data."

Alexander said his policy on inspection of farmers' tax returns by Agriculture Department officials was to limit access to names and addresses. The sub-committee recommended that no personal financial data from the returns should be provided unless individual taxpayers gave their voluntary consent "in writing."

"Ideally," the sub-committee said, "the farmers could provide this information directly to the Department of Agriculture."

The IRS says that in the first half of 1970 it made 14,000 tax returns available to the Department of Justice and Labor, the Federal Communications and Securities, the Exchange Commissions, the Federal Home Loan Bank, Renegotiation, the National Labor Relations Board, the Small Business and Social Security Administrations and the Post Office Department.

The House Ways and Means Committee is expected to start hearing soon on a series of bills to protect tax returns sponsored, among others, by Reps. Jerry Litton, D., Mo.; Charles Thone, R., Neb.; Jack F. Kemp, R., Buffalo; and Barber B. Conable, Jr., * * * Alexander.

[From the Watertown (N.Y.) Daily Times, Mar. 5, 1974]

BUTZ SAYS FARMERS' INCOME TAX RETURN INSPECTION IS A JUDGMENT MATTER

(By Alan Emory)

WASHINGTON.—Agriculture Secretary Earl L. Butz says it is "essentially a matter of judgment" whether his department's inspection of individual farmers' income tax returns "involves invasion of privacy."

Butz made the comment in a letter to Rep. William S. Moorhead, D., Pa., chairman of a House Government Operations sub-committee. The sub-committee had asked Butz to shelve using the access to the tax returns until after it had completed its inquiry into the issue.

President Nixon last year issued an executive order allowing the income tax inspection without any public notice or hearing. It was published in the Federal Register.

The Justice and Treasury Department say it was designed as a model for all the executive agencies.

Ironically, when former Agriculture Secretary Clifford M. Hardin originally requested, in 1970, certain farm data that could be matched with names of farm operators obtained from sources outside the Internal Revenue Service he said specifically he was not seeking an examination of individual tax records.

Butz told Moorhead in June, 1973, that "no employee" of his department would examine any individual tax return under the authority of the Nixon order, but he refused to put the authority in cold storage.

"The list development procedure we have in mind is clearly in the public interest," he insisted.

In July he told Moorhead that the "effectiveness of the security handling of data" by the staff of his Statistical Reporting Service "has not been challenged."

PAARLBERG COMMENTS

Don Paarlberg, director of agricultural economics for the department, said the department had never sought the inspection authority and maintained the original draft had been broadened during reviews by the Treasury and Justice Departments.

Last June Assistant Attorney Gen. Robert G. Dixon, Jr., said, "The original order was prepared by the Department of the Treasury in language designed to serve as a prototype for future tax return inspection orders."

A modified order, he said, was "approved as to form and legality."

Paarlberg conformed the broad intent of the order by declaring, "We understand the first order was designed as a model to be used by other departments."

According to Rep. Jerry Litton, D-Mo., author of a bill-tightening procedures for inspecting individual tax returns, even the revised Nixon order leaves a farmer's return "an open book."

It authorizes examination of tax returns to obtain any information so long as it can be construed to mean "a measure of size of the farming operation of the taxpayer," he said in a letter to the House Ways and Means Committee.

Rep. Charles Thone, R-Nebr., author of another tax return safeguard bill, says there would be a lot less exposure of returns if the Agriculture Department obtained its statistical data from the Census Bureau as authorized by the White House.

At one point in last year's hearings, Paarlberg commented, "We do not care which department they come from."

"I do very much," Thone snapped back.

Litton, who was curious as to why Nixon had issued the order if the Agriculture Department had not asked for it, recalled that when it was being worked up, a couple of Watergate figures were active in the Treasury Department.

One was G. Gordon Liddy who master-minded the break-in of Democratic National Committee headquarters and had been employed in the office of general counsel, and another was John Caulfield, who was a staff assistant to the

assistant treasury secretary for enforcement and then director of enforcement of the Bureau of Alcohol, Tobacco and Firearms.

A third Watergate figure, former Presidential Counsel John Dean, had recommended the Internal Revenue Service zero in on political targets by making a requested audit "of a group of individuals having the same occupation."

Under questioning by Rep. Bill Alexander, D-Ark., who helped uncover the executive order and trigger last year's hearings, Paarlberg said he was not sure whether the decision not to publish the order or announce it publicly had come in a phone call from the Treasury Department "or whether it came from the President's staffman." He said he had been in touch with both.

He said, however, he had not talked to indicted Nixon aides H. R. Haldeman and John D. Ehrlichman.

Alexander said that blanket authority to inspect individual tax returns of any group, as the Nixon order provided, "clearly constitutes an invasion of the right of privacy of that group."

"Is this evidence of a master plan of the federal government to oversee the private affairs of every group of citizens?" he asked in his latest newsletter to constituents.

He raised the possibility that it might open the door for eventual Commerce Department inspection of returns of homeowners receiving Federal Housing Administration-insured loans, Labor Department inspection of returns of wage earners and Health, Education and Welfare Department inspection of returns of doctors and teachers.

Mr. GOLDWATER. Mr. Speaker, I thank the gentleman for his words.

I would like to add that the gentleman along with his colleague, the gentleman from Nebraska (Mr. Thone) were very instrumental in persuading the White House that this was in fact a bad move and a direct question of personal privacy. I think the general public owe the gentleman from Missouri (Mr. Alexander) and the gentleman from Nebraska (Mr. Thone) a debt of gratitude for getting this order rescinded.

Mr. ROUSSELOT. Mr. Speaker, will the gentleman yield?

Mr. GOLDWATER. I yield to the gentleman from California (Mr. Rousselot).

(Mr. ROUSSELOT asked and was given permission to revise and extend his remarks and include extraneous matter.)

Mr. ROUSSELOT. Mr. Speaker, I appreciate having the opportunity to join with my colleagues in an expression of concern about the congressional commitment to privacy. This commitment is rooted in the oath of office we take swearing to uphold the principles of the Constitution. Unfortunately, many of the legislative proposals we have approved in recent years have ignored this basic right of American citizens, and I believe it is important that we discuss here today the meaning of this responsibilty, and how we, as legslators, can regain the confidence of the Nation by affirming our commitment.

My discussion will be limited to specific areas which are related to my committee assignments on the Post Office and Civil Service Committee and the Banking and Currency Committee.

CENSUS AND STATISTICAL DATA

First. Congressional commitment to privacy and the census. In recent years, many Members have expressed concern that the very nature of the personal questions asked in a decennial census violate the privacy of American citizens. As ranking minority member of the Census and Statistics Subcommittee, I share this concern. The mandatory questions being asked on census forms probe extensively the most intimate details of Americans' lives and gor far beyond the constitutional intent of the census—to count the people in order to determine congressional districting. The subcommittee plans to undertake an in-depth study of laws and regulations relating to the confidentiality of statistical data collected by government agencies, and I fully endorse this effort.

Last week the subcommittee concluded hearings on legislation relating to congressional approval of the content of economic census questionnaires. The questions asked in an economic census or in a decennial census may constitute just one form of invasion of privacy. In testimony before the subcommittee, Congresswoman Edith Green brought out that another important concern is that the paperwork burden which is imposed on American citizens by their Government is in itself an invasion of privacy and an intrusion of the lives of our citizens. The economic census—a questionnaire that is completed in its entirety over a 2-year period—being just on example. We also have Occupational Safety and Health Act reporting requirements, wage and price control reporting requirements, IRS reporting requirements—the list is endless, Mr. Speaker. The

paperwork burden required by the legislation we approve is an important factor which is often overlooked, and demonstrates that our commitment to privacy goes far beyond obvious considerations.

BANK SECRECY

Second. Congressional commitment to privacy and the banking industry. In connection with our responsibilities as members of the Banking and Currency Committee, Congressman Clair Burgener and I introduced a bill last session, H.R. 10021, the Right to Financial Privacy Act. This legislation is designed to protect the constitutional rights of citizens of the United States, and to prevent unwarranted invasions of privacy by prescribing procedures and standards governing the disclosure of financial information by financial institutions to Federal officials or agencies. I believe this legslation is necessary to preserve the confidential relationship between financial institutions and their customers and the constitutional rights of these customers. Enactment of this bill would insure that the individual has the same rights of protection against unwarranted disclosure of records maintained in the financial institution as he would have if these records were maintained in his own possession.

The bill we introduced would allow the disclosure of a customer's records only if: the customer specifically authorizes the disclosure; the financial records are disclosed in response to an administrative subpena or summons providing the individual is notified by certified mail and directs the financial institution to comply, or the financial institution is served with a court order directing it to comply which is issued after the customer has been notified and has an opportunity to challenge the subpena or summons; a search warrant is obtained by the Federal official or agency which is served in both the customer and the financial institution; or a judicial subpena is issued with a copy being served on the customer and 10 days pass without notice that the customer has moved to quash the subpena.

Similar financial privacy bills have been introduced in the House but the Rousselot-Burgener bill differs in that it does not preempt State and local laws regulating disclosure of customer information. Like legislation to govern actions by State and local officials and agencies has passed the California State Assembly and is now pending before the California State Senate. It is entirely possible that State legislative bodies might also wish to establish such regulatory controls as are appropriate to their individual requirements. H.R. 10021 would regulate only those actions of Federal officials and agencies. Other financial privacy bills extend the regulating provisions to also govern actions by State and local officials and could possibly be in conflict with States' rights.

Also, other versions would only allow a financial institution to notify law enforcement officials of violations of criminal law suspected of being committed against the financial institution itself. The Rousselot-Burgener bill recognizes that in some rare instances the financial institution could have reason to suspect other violations of criminal law.

Passage of this legislation would be an important step in assuring an individual's right of privacy, and I urge my colleagues to review this important bill and consider it favorably when it comes before this House for vote.

Another instance where the banking system has been used as a tool to invade the privacy of American citizens is the Bank Secrecy Act—Public Law 91–508. Yesterday the U.S. Supreme Court handed down a ruling, and by a vote of 6 to 3 upheld the constitutionality of the domestic reporting and recordkeeping requirements in title I of this act. In dissent, Associate Justice William O. Douglas argued, and rightfully so, that this act has "saddled upon the banks of this Nation an estimated bill of over $6 million a year to spy on their customers." Justice Douglas further made the point that, "Unless we are to assume that every citizen is a crook, an assumption I cannot make," it is "sheer nonsense" to claim that every citizen's bank records are important in tax and criminal investigations.

Mr. Speaker, we in Congress are responsible for the Bank Secrecy Act which I believe does, in fact, violate the constitutional rights of the citizens of this Nation. In connection with the Supreme Court ruling yesterday, Associate Justice William Rehnquist to agreeing with the decision has reportedly said, "that depositors must wait until their records are seized before they can claim in court that their privacy rights are threatened. He did not rule that banks must notify their customers nor did he guarantee success for the customers when they do go to court." This statement emphasizes the need for the Congress to take action immediately, not only to repeal the provisions in title I which require the Ameri-

can banking system to spy on its customers, but to also enact my bill, H.R. 10021, to protect a customer's privacy.

The California Bankers Association was involved in initiating this challenge to the Bank Secrecy Act. They have effectively stated the unconstitutional provisions in the act in their brief which was filed with the court, and I believe that every Member who is concerned with our commitment to privacy will be interested in the following excerpt from this brief summarizing the arguments.

[The excerpt follows:]

SUMMARY OF ARGUMENT

(1) The announced purpose of the Bank Secrecy Act is the recording and retention of bank records having "a high degree of usefulness in criminal tax or regulatory investigations or proceedings." The Act and implementing regulations, in alleged pursuit of that purpose, require banks to monitor *every* bank account in the United States, and to copy and retain virtually every piece of paper that passes through the American banking system. As a result, and since the checks one writes reveal the intimate details of a citizen's financial, social and political life, banks are being forced to compile an exhaustive profile on virtually every adult member of the American community.

(2) There is almost no relationship between the Bank Secrecy Act's basic purpose—the detection, apprehension and conviction of criminals—and the requirement that virtually every piece of paper passing through all 200 million American bank accounts be copied and retained. Even if one were to assume that every crime committed in the United States would somehow be revealed by the perpetrator's bank account—including those such as homicide and forcible rape that have little or nothing to do with banks and banking—*less than 4.4%* of the bank accounts in the United States would be involved. Quite apart, then, from all other objections, the wholesale surveillance of every bank account in the United States is a witless enterprise.

(3) The indiscriminate, mass surveillance of every bank account in the United States is unnecessary and inappropriate. There are any number of alternate, reasonable means available. As such, the Bank Secrecy Act violates due process. See, e.g., *Helvering* v. *City Bank Farmers Trust Co.*, 296 U.S. 85 (1935) and *N.A.A.C.P.* v *Alabama*, 337 U.S. 288 (1964).

(4) The Act violates the Fifth Amendment right of due process by imposing two separate and unreasonable requirements on the American banking industry.

First, the Bank Secrecy Act plainly violates the limitations this Court has imposed on compulsory recordkeeping. There is virtually no relationship between the objectives of the Act and the mass surveillance of every bank account in the United States. The records required have no specific purpose. They have *nothing* to do with the regulation of banks and the banking business. They destroy the Fifth Amendment limitations this Court has imposed on the use of required records against the recordkeeper. See, *Shapiro* v. *United States*, 335 U.S. 1 (1948); *Marchetti* v. *United States*, 390 U.S. 39 (1968); *Grosso* v. *United States*, 390 U.S., 62 (1968).

Second, the Act violates economic due process by requiring banks to spend approximately $6.1 million each year to make and retain records they do not need or want—$6.1 million a year to spy on their customers.

(5) In *United States* v. *Powell*, 379 U.S. 48 (1964), *Donaldson* v. *United States*, 400 U.S. 517 (1970) and *Couch* v. *United States*, 409 U.S. 322 (1973), this Court set forth various safeguards against the unlawful use of the governments summons and subpoena power against third-parties. By requiring banks, among others, to record and retain writings that would otherwise belong to the maker (e.g., checks deposit slips, etc.) the recordkeeping required by the Bank Secrecy Act transfers title and possession to the banks. This destroys the practical and legal ability of a citizen under investigation to assert the Fourth and Fifth Amendment rights outlined in *Powell*, *Donaldson* and *Couch*.

(6) The privacy and anonymity protected by the First Amendment includes the confidentiality inherent in bank-customer relations. By allowing the Treasury Secretary unlimited discretion to include or exclude banks and bank accounts from its recordkeeping requirements, the Bank Secrecy Act violates the rule that intrusions on First Amendment rights be narrowly drawn, reasonable and definite. See, e.g. *Niemothko* v. *State of Maryland*, 340 U.S. 268 (1951).

(7) The wording of the Bank Secrecy Act and the government's arguments to this Court confirm that the recordkeeping provisions are the handmaiden of the Act's automatic reporting requirements. Since the reporting requirements plainly violate the First, Fourth and Fifth Amendments, the Act's recordkeeping provisions are unconstitutional for the same reasons.

(8) Finally, since its members are being injured, the California Bankers Association has standing to assert their constitutional rights (*Sierra Club* v. *Morton*, 405 U.S. 727 (1972)). In addition, the CBA has standing to assert the constitutional rights of its members' customers. Those rights are fundamental and the banks appear to be the only parties affected by the Act's recordkeeping requirements in a position to assert this constitutional challenge. See *Eisenstadt* v. *Baird*, 405 U.S. 438 (1972).

In conclusion, Mr. Speaker, I sincerely hope that we can start a new trend in Congress. A trend that will result in our protecting American citizens' privacy instead of violating it, a trend that can only be accomplished by less Federal control and intervention.

Mr. GOLDWATER. I thank the gentleman. He is absolutely right. It is time for the farmers and the American people to review this procedure, to look where we are going. The technological age has brought many rapid advances in many areas of our lives. One of the great areas is in the multitudinous use of computer technology to record information about individuals.

It reminds me of the same situation that occurred with supersonic transportation. At one time we were building supersonic transportation at such a rate until we had to stop and say, "Where are we going? What effect does this have on human life?"

I think we have to do that in the area of computers in this technological age and stop and say, "Where are we going in our personal lives?"

This commitment by the Congress is a good one. I congratulate my colleague for his contribution in his area of expertise.

Mr. ROUSSELOT. Mr. Speaker, will the gentleman yield further?

Mr. GOLDWATER. I yield to the gentleman from California.

Mr. ROUSSELOT. I know the gentleman has worked long and hard on this subject. It has taken some time for all the Members to gather together the information on this sweeping matter of rights.

Mr. GOLDWATER. Mr. Speaker, if I might also mention to my friend, the gentleman from California, not only his interest in the census data, but the fine contribution of a former colleague, Mr. Jackson Betts, made many years prior to our involvement. Certainly he paved the way and aroused our interests and our concern. I think we all owe him a compliment for his contribution.

Mr. LAGOMARSINO. Mr. Speaker, will the gentleman yield?

Mr. GOLDWATER. I yield to my friend and colleague, the gentleman from southern California (Mr. Lagomarsino).

(Mr. LAGOMARSINO asked and was given permission to revise and extend his remarks.)

Mr. LAGOMARSINO. Mr. Speaker, I commend my very good friend and colleague from California and from my own county, Mr. Goldwater; Mr. Koch, the gentleman from New York, and others who are bringing this special order to our attention and allowing us to participate in it. I do not think there is any subject the American people are more concerned about and want us to do something about than this question.

Mr. Speaker, more than 2,400 years ago, the Greek orator Pericles noted that one of the hallmarks of a free society is "mutual toleration of private conduct." The common law precept that a man's home is his castle, finds expression in the English Magna Carta. And our own Constitution guarantees the right of the people to be secure in their persons, houses papers, and effects.

Despite this admirable, and nonpartisan, historical commitment to privacy as a prerequisite of free society, we find ourselves today facing a very real threat to this right. The challenge comes not from without, but from within. Our own technology threatens to render the guarantees of our constitution useless. And unless we act now, just as our forefathers did and their fathers before them, we may find ourselves the slaves rather than the masters of our modern information systems.

Mr. Speaker, I have some Greek antecedents, but I have more Roman blood, and I remember from my history books what happened when the Roman Empire became tophéavy with bureaucracy and red tape. It collapsed of its own weight, and became ripe pickings for renegades. This issue is not a partisan issue. It transcends ideologies. It goes to the root of what governments are created to do. Our Republican form of Government was created to do those things that the people find difficult to do for themselves, and no more. The people, whom we serve, have reserved to themselves all other rights and authority. And when Government, or any private group, gains such power over the private conduct of its citizens that by its very operation it threatens their security, then it is time to act.

The people of California 2 years ago enacted an amendment guaranteeing their right to privacy. I believe they did this, not because they wanted an increase in criminal activity, obviously, but because they wanted a decrease in governmental activity. In our society, where an honest man's word is his reputation, where a presumption of innocence is the law, perpetual surveillance is anathema. And when it is conducted on a pervasive scale, often without even the knowledge of the people or an opportunity for challenging an individual dossier, then the time has come to sound the alarm.

I believe the Congress should act now to renew the commitments made in the Constitution and in our laws for the right of free citizens to be secure. Secure in their persons, in their houses, papers and effects, and in their private lives.

If we do not make this commitment, if we do not act now to gain control over the paper bureaucracy, public and private, which is beginning to pervade our lives, we will wake up, 2,400 years after Pericles set out the limits of Government interference in private affairs, in the year 1984. Let us pray that day never comes.

Mr. Speaker, my colleague from California (Barry M. Goldwater, Jr.) is working steadfastly to restore rights of privacy in America. He recently spoke before a seminar sponsored by the National Bureau of Standards. I include his remarks.

[The remarks follow:]

SPEECH BY CONGRESSMAN BARRY GOLDWATER, JR. TO NATIONAL BUREAU OF STANDARDS COMPUTER SECURITY CONFERENCE

A distinguished former colleague of mine, Congressman Jackson Betts, who was one of the pathfinders in promoting legislation to protect privacy, once said: "Privacy is not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves."

I am pleased to be a congressional participant in the conference sponsored by the Institute for Computer Sciences and Technology, here today.

Since coming to Congress almost five years ago, I have become increasingly concerned about the growing menace privacy invasion poses to the American citizen.

Early last year, I decided to initiate certain proposals to assure the American citizen that he would indeed have control, as mentioned by Congressman Betts, over information compiled and retained about him.

An initial report was to work very closely with the Secretary of Health, Education, and Welfare prior and after the release of the very extensive HEW study entitled "Records, Computers, and the Rights of Citizens". This report was released last July.

I am most impressed with this study, and in order to carry out its specific recommendations, I introduced two bills.

One, "The Freedom of Information Act", H.R. 11275, is basically aimed at accomplishing the following three objectives:

(1) To guarantee individuals the right to find out what information is being maintained about them in computerized systems and be able to obtain a copy of it upon demand.

(2) To allow a person to contest the accuracy, pertinence, and timeliness of any information in a computer-accessible record about him.

(3) To require record-keeping organizations to inform individuals on request of all uses made of information being kept about them in computerized files.

Shortly after introducing this bill, I joined with Massachusetts Governor Francis Sargent, Senator Edward Brooke, and Congressman Michael Harrington, in an administrative petition with the Justice Department, which asked former Attorney General Elliot Richardson to terminate operation of the F.B.I. administered offender files, which are a part of the National Crime Information Center, until he has issued formal regulations to safe-guard the rights of individual citizens.

Additionally, I introduced a bill to amend the Social Security Act, that would give each individual in this country the right to refuse to disclose his or her social security number. Then too, organizations with the authority to use the number would be prohibited from disclosing the number to organizations that lack such authority.

This legislation is designed to prevent the social security number from becoming a "standard universal identifier" that can be used by computers to track all the errors, omissions, and/or sins of an individual from cradle to grave.

Other actions included the introduction of legislation to require consumer reporting agencies to allow a consumer to inspect credit records, legislation to protect individuals from statistical reporting systems, and a bill to establish a Select Committee on Privacy in the House of Representatives.

Recent events indicate that more and more people are becoming concerned about privacy invasion. This is a good sign, because I have always maintained that the worst enemy of privacy is not the computer—its worst enemy is apathy and ignorance.

I am pleased that the President addressed himself to privacy in his recent state of the union address. Just a few days ago, he announced the formation of a commission on the issue of privacy and data banks in our country.

Suffice to say, it does us little good to attack the computer—it is only an instrument of man. What must be attacked is the computer mentality—the kind of faceless bureaucracy in and out of government that seeks to make the computer a supreme being.

The potential of privacy invasion is always present in a sophisticated computer operation. Remarkably, the misuse of information held about individuals in computer systems has been held to a minimum. But the potential for misuse is still there, and certainly data surveillance has grown to very menacing proportions due to the technological advances which alter such information to be given multiple use and consolidation through automated systems.

Substantial increases in demand for personal reports by government agencies, private systems, and social science researchers have intensified the severity of the problem.

As you know, it is not enough for us to discuss the technology of the computer and speak of privacy in an abstract fashion. We must resolve, at this conference, and in every other private and public forum to do what is necessary to protect our constitutional right to privacy.

Let us make no mistake about it, the computer already knows more about most of us than we know about ourselves. The amount of data held in computer systems is enormous. Think about it for a moment. The list includes tax returns, census responses, social security data, military records, security files, finger prints, FHA and VA mortgage guarantees, credit records, health data, and social research involving individuals. Such examples are barely the tip of the iceberg.

I say tip of the iceberg because everytime Congress passes legislation giving the Federal Government added responsibilities and power, more paperwork is created and consequently more information is known about the individual citizen.

Of course, this is a sobering thought, but what can we do about it?

Initially, we must understand our right to privacy and how important it is to protect this right. Secondly, we must rely on wise laws that protect our privacy rights.

We must remember that our citizens give the government personal information on what should be on a confidential basis and for a specific purpose. Americans deserve the assurance that this information will not be used for any other purpose in the future. But, do we have this assurance? Not necessarily, I fear.

Several years ago a House Congressional Committee discovered that the confidentiality of Government files is a myth. Such files sometimes float from agency to agency. Federal investigators in some instances are given access to information far removed from the subject of their inquiry. Folders sit open for inspection on desks and in the "in" and "out" baskets of many government offices. Outright "leaks" of information occasionally come a light.

Of course, this is interesting, you say. But, then you add that the government has never mis-used the information about you, so why worry? But, I submit that this may not be the case in the future unless we begin to embark on a course to make certain that it will not be misused.

It is always possible for unscrupulous men in high places to apply unethical standards to the use of confidential information. One of history's leading examples is the detailed European census that was in effect long before the advent of Hitler. Tragically, this census provided a convenient and efficient tool for Nazi use in many European nations. In some countries like Czechoslovakia, statistical data already available facilitated the Nazi takeover.

Impossible here? Not necessarily. Erroneous data or information, whether computer-stored or not, can lead to bizarre occurrences that constitute a blatant invasion of privacy.

Two years ago 15 men wearing beards and dirty clothes took a battering ram and knocked down the door of a *suspected* violator of a Federal gun law. Did this happen in Soviet Russia? No, it happened near Washington, D.C. The suspect was a law-abiding citizen, who only collected harmless antique weapons. He is now totally paralyzed—his life is in shambles. The ruffians who perpetrated this crime? They were officials of the U.S. Treasury Department, and they broke into the victim's home on faulty information that he was in violation of the 1968 Gun Control Act.

This is not a remote example. Earlier this year, the same thing happened to a family in Winthrop, Massachusetts. A couple and their daughter, who was ill, were awakened in the middle of the night when state and Federal lawmen broke down two doors to their home on a narcotics raid. The policemen had entered the wrong home.

Of course these are clear-cut examples of private invasion. There should be no question that they also violated the fourth amendment to the constitution.

But, there are other examples almost as sinister in nature. I have received numerous letters from American citizens describing examples of data bank and Social Security number abuse. Each letter seems to detail a new horror story worse than the one before. Some of the letters have actually come from computer systems analysts in the field of data processing.

The protection of personal files in all data systems deserves immediate attention on the part of both the government and the private sector. I would like to challenge this conference to not only exchange ideas and make recommendations to assure the privacy of individual data subjects in computer operations, but I would like to see a definitive statement emanate from this conference calling for a restoration of freedom of privacy.

It is not difficult to determine the adverse potential of today's technology on our right to privacy. What is difficult is making certain our traditional liberties and beliefs can be secure against growing technological onslaughts against privacy.

Mr. GOLDWATER. Mr. Speaker, I thank my colleague from California (Mr. Lagomarsino) and recognize him for the contributions he has made to this issue and his concern while he served in the State House in California.

Mr. EDWARDS of California. Mr. Speaker, the day of Big Brother and constant surveillance is already upon us. Regularly we read or hear about a new Government program that necessitates the gathering of some new information on certain individuals or class of individuals. One's social security number is not longer just used in the administration of social security benefits as it was originally intended. It has become the identifier for almost every citizen in this country: it is used on driver's licenses, banking applications, school applications—in some schools grades are dispensed by social security number—all credit applications, and a host of other documents that one signs in their daily lives. Only this past Sunday in the Parade section of the Washington Post was the reading public informed about the extent of unsubstantiated information that goes into school records. We were also informed by that same article that law enforcement agencies, military agencies or other agencies of authority are given unfettered access to these records upon request.

The intrusion upon privacy of the citizens of this country has been slow and unobtrusive for the most part to this point. The agencies collect a little more information today, a little more information tomorrow, and pretty soon there is a complete dossier on every individual in this country. The irony of this situation is that the individual on whom this information is collected is not allowed to review the records and to challenge the information. The files are transmitted freely throughout the country and very important decisions affecting the future of these individuals are made with unblinking eye and unquavering hand. It is too easy to deny a person an education because he was arrested when he was 16 years old. It is too easy to stop one's insurance coverage on his car because he keeps a dirty house. It is too easy to deny housing to someone because his previous neighbor said that he had loud parties. It is too easy to make a decision without checking on the facts. And as each day passes more and more people are being caught in a record prison unable to free themselves even with the truth.

The situation now becomes even more insidious with the dawning of the age of the computer. Proliferation of computer data banks, investigatory agency upon investigatory agency is almost a seamless web of Government intrusion upon the individual. The problem is becoming acute. The technological advances in computer science develop not only an ease in obtaining information but also an in-

satiable appetite by public and private industries to collect every possible piece of knowledge on every possible citizen. The abuses to our right of privacy are excessive. Unfortunately the practice of collecting extensive information on our citizens has gone unquestioned by the American public. It has been only in recent years that some of our citizens have become appalled by this massive collection mania for information. The problem will not be alleviated by the waving of some magic wand in Congress. We cannot correct all the abuses with one piece of legislation. Each individual kind and type of abuse will have to be found and dealt with by a separate piece of legislation. In this manner, we begin to seal the loopholes through which public and private agencies spy on the citizens of this country.

The Subcommittee on Civil Rights and Constitutional Rights of the House Committee on the Judiciary, of which I am chairman, have spent over 2 years studying the abuses caused by the dissemination of arrest records and other criminal justice information. In 1971 I introduced H.R. 13315, a bill that proposed to regulate the dissemination and use of criminal arrest records. An arrest record or "rap sheet" is simply a sheet on which notations of arrests are made and most frequently do not even carry the disposition of the charge. According to FBI statistics, law enforcement agencies make some 8.6 million arrests per year for all criminal acts, excluding traffic offenses. Of these arrested, approximately 4 million are never prosecuted, or have the charges dismissed. Yet, these 4 million arrests annually are inserted on individuals "rap sheets" and become a part of what is considered criminal records. Unfortunately, these arrest records when circulated are treated much the same as a conviction record. There is no evidence yet presented that a person arrested and never convicted is any more of a job risk, credit risk, tenant risk or student risk than any other citizen. Yet every police agency, school, credit corporation, prospective empolyer and all other public and private agencies want desperately to have knowledge on arrest records as though it provides a certain and revealing insight into a person's character. These raw criminal arrest records time and time again reach out and injure people who have never been involved in any illegal or criminal act and their use is widespread.

During our extensive hearings on arrest records we became aware of the existence of the National Crime Information Center maintained at the national level by the Federal Bureau of Investigation. Members of the subcommittee toured the National Crime Information Center's facilities and viewed its operation. The NCIC is part of a telecommunications system throughout the country that connects potentially all law enforcement agencies with each other. This system permits the rapid exchange of criminal information with any inquiring law enforcement agency. The NCIC itself began by collecting information on stolen items and wanted persons. But since its inception that part of the NCIC that deals with active criminal offender records has grown and is continuing to grow. These computerized criminal histories are searched as a part of identification service that the FBI provides for agencies of Federal and State governments and other authorized institutions, including savings and loan associations and national banks, which seek information on an individual's arrest record for the purpose of empolyment clearances and licensing. I personally was somewhat shocked at the time of my viewing these installations to find that there were no statutory parameters that guide the operations of the dissemination of criminal information; they were operating on a statement of principle promulgated by its advisory policy board. As if this was not frightening enough, I became aware that the advisory policy board is made up entirely of criminal justice officials. This dramatically points up the inherent confict of interest in allowing this massive system that affects the lives of every citizen of the United States to regulate itself. We have always maintained and our Constitution requires civilian control over the military—this constitutional analogy should not be lost here.

With the knowledge of this massive national computerized system exchanging information throughout the country, I introduced in August of 1973 H.R. 9783 that would provide for the protection of the right of privacy in the dissemination of criminal justice information. Earlier this year our subcommittee added to its consideration Senator Ervin's comprehensive bill on criminal justice information systems and the Department of Justice bill dealing with the same subject. We have since held several days of hearings on these three bills. Our witnesses have included the Attorney General of the United States, William Saxbe, the Director of the Federal Bureau of Investigation, Clarence M. Kelley, Mr. Arnold Rosenfeld, the Director of the Massachusetts Criminal Histories Systems Board and representatives of the Department of Defense, the Civil Service. Much knowledge

has been imparted to the members of our subcommittee in this very complex and threatening area. It has become apparent with each passing day that congressional regulation and oversight in this area is mandated. We can no longer wait for self regulation by these agencies, public and private, nor for the system to work itself out. We must move on every front to shore up the rights of privacy of the citizens of this country against the ever encroaching threat of the massive accumulation of unrestricted information.

Justice Brandeis noted many years ago that the makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They sought to protect Americans in their beliefs, their thoughts, their emotions, and sensations. They conferred as against the Government the right to be left alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustified intrusion by the Government upon the privacy of the individual, whatever means empolyed, must be deemed a violation of turning the tide against Big Brother and constant Government surveillance and perhaps even the Constitution itself, we now have the awesome obligation of turning the tide against Big Brother and constant Government surveillance which is already upon us.

Mr. BROWN of California. Mr. Speaker, poetry can often bring the levity required to see the deeply sensitive human situation we are talking about when we speak of rights of privacy. Under the all-knowing hand of a technocratic state, our cemeteries may well be lined with headstones with personal identification numbers rather than names chisled on them. A message from such an era comes in the form of this poem by W. H. Auden.

[The poem follows:]

THE UNKNOWN CITIZEN

(To JS/07/M/378 this marble monument is erected by the State)

He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned world, he was a saint,
For in everything he did he served the Greater Community.
Except for the War until the day he retired
He worked in a factory and never got fired,
But satisfied his employers, Fudge Motors, Inc.
Yet he wasn't a scab or odd in his views,
For his Union reports that he paid his dues,
(Our report on his Union shows it was sound)
And our Social Psychology workers found
That he was popular with his mates and liked a drink.
The Press are convinced that he bought a paper every day
And that his reaction to advertisements were normal in every way.
Policies taken out in his name prove that he was fully insured.
And his Health-card shows he was once in hospital but left it cured.
Both Producers Research and High-Grade Living declare
He was fully sensible to the advantages of the Instalment Plan
And had everything necessary to the Modern Man
A phonograph, a radio, a car and a frigidaire.
Our researchers into Public Opinion are content
That he held the proper opinions for the time of year;
When there was peace, he was for peace;
when there was war, he went.
He was married and added five children to the population,
Which our Eugenicist says was the right number for a parent of his generation,
And our teachers report that he never interfered with their education.
Was he free? Was he happy? The question is absurd:
Had anything been wrong, we should certainly have heard.

Mr. GIAIMO. Mr. Speaker, the right to be left alone—the right to privacy—is one of our most fundamental and cherished rights. Yet this right is constantly being eroded by computer data banks, copying devices and other products of a refined technology. In short, invasion of privacy has become another word for efficiency, as Government and business seek to learn more about individual citizens than they have a need or right to know.

We are all familiar with wire-tapping, official eavesdropping and political spying. But let us not forget the more subtle forms of invading someone's pri-

vacy. Unauthorized financial disclosure by banks and other institutions, the release of telephone and business records, the denial of rights of access to information collected on an individual, the selling of mailing lists, the abuse of credit ratings, the expanded use of social security numbers as an identification reference, the use of mandatory census questions, unsolicited commercial telephone calls—all these practices are an infringement of the right of privacy.

Congress must compose a legislative response to this wholesale invasion of individual privacy, at the same time balancing the right to be left alone against the proper needs of society. Nineteen eighty-four, only a decade away, must not be a target date for fulfilling George Orwell's chilling prophecy of an all-regulated society. Private lives are private affairs. Public freedoms have little meaning when personal liberties are diminished.

We need legal safeguards to eliminate indiscriminate public use of an individual's telephone, school, army and bank records, to name a few. The privacy of these records must be guaranteed to prevent the unscrupulous from misusing the information they hold. Individuals must have the right to inspect records concerning them to held by federal agencies and private businesses. A means must also be devised to allow individuals to correct these records if they contain erroneous or misleading information. I am one of the original sponsors of H.R. 8375, legislation that would do precisely this, and I am pleased to note that the Government Operations Committee has held 2 days of hearings on this and similar bills. I urge my colleagues to act favorably on this measure when it is reported to the House floor.

This legislation is only the beginning of what we need to do. The task is enormous, for ultimately we must inspect the inspectors. But it is a task worth pursuing, and necessary to pursue. We must stop Big Brother.

Mr. MELCHER. Mr. Speaker, the late author George Bernard Shaw, in a speech in New York in 1933 said:

"An American has no sense of privacy.

"He does not know what it is.

"There is no such thing as privacy in this country."

We have come a long way since then. It is hard for me to imagine what Mr. Shaw would be saying if he were alive today and could see the mistrust and the indignation of our citizens that have developed in the last few years as computers have recorded and stored information on every facet of our private lives for any one of a hundred purposes. It is clear to me that the American people have a very real sense of privacy which they now see as being threatened as never before—whether by businesses wanting to know whether a person deserves a credit card, or by Government officials wanting the Internal Revenue Service to become more "politically responsive" by taking a closer look at tax returns of those on "enemy" lists.

I am pleased to speak today in support of a renewed congressional effort to protect the rights of our citizens to the privacy they want and deserve.

The greatest potential for invasion of privacy is that of Government, whether through conscious policy decisions or by actions of overzealous individuals. A shocking example of this is Executive Order 11697 issued by President Nixon in January of 1973. That order, which the administration refused to rescind until a few days ago when it bowed to congressional pressure, would have granted broad authority for the opening up of Internal Revenue Service taxpayer returns and files on 3 million farmers to the Department of Agriculture, supposedly for statistical purposes. The sinister part of the order is that it was drafted by the Treasury Department, over objections of the Internal Revenue Service, to serve as a model for allowing other Government agencies to have access to private income tax information.

In view of recent exposure of attempts to use the IRS politically, the implications are frightening. For this reason I have joined with Mr. Litton and other concerned Members in sponsoring legislation (H.R. 12349) to strictly limit disclosure of information gathered by the Internal Revenue Service. That disclosure would be allowed only to appropriate Government representatives for tax administration and law enforcement purposes. Legislation such as this is vitally needed to prevent abuses of power by Government and to protect our right to privacy—to make sure we have no future fights over Executive orders such as 11697.

Another less sinister, but perhaps as far-reaching threat to our privacy is that of the credit reporting companies and systems. Here the problem is probably more a matter of mistakes and information misinterpretations stored in a computer that come back to haunt a citizen applying for credit or even a job. When

credit is denied or a job given someone else, the person may never know that he was the victim of a computerized sandbagging job. We have made some progress in requiring that credit information compiled about a person be disclosed upon request and an opportunity be given for correcting that information. But more should be done.

Congress has made progress at attempting to assure the American people their right to privacy. But we must continue to work at it. I am sure George Bernard Shaw would have liked someone to prove him wrong—about lack of privacy for Americans, and Congress should demonstrate that there is such a thing as individual privacy in this country—and that it must be preserved and protected.

Mr. SEIBERLING. Mr. Speaker, in recent years hundreds of thousands of veterans have been unfairly subjected to an invasion of privacy by the Defense Department's policy of placing certain highly prejudicial information on their discharge papers. This information specifies what the Defense Department calls the "reason for separation" from active duty and is known as a "separation program number"—SPN—which appears usually in coded form.

In fact, the information has almost nothing to do with the reason why an individual is discharged. Instead, it represents an attempt by DOD to classify the character of service beyond what is permitted by the classification of types of discharge—honorable, general, undesirable, bad conduct, dishonorable. The SPN may classify the veteran as a drug abuser, alcoholic, shirker, liar, bed-wetter, homosexual, sexual deviant, or simply as an "antisocial' person.

The use of a classification system containing SPN's constitutes more than an invasion of individual privacy by the Defense Department. The system makes it possible for private employers to gain access to personal and perhaps unfounded information about job applicants. Placing an adverse SPN on an individual's discharge papers can make it impossible for him to obtain a job, even if he has an honorable discharge.

Last year I conducted an investigation of corporate employment practices concerning veterans, especially those with less-than honorable discharges. The results are summarized in the Congressional Record of November 28, 1973. My investigation showed that there was massive employment discrimination against veterans with less-than-honorable discharges. Over 40 percent of the Nation's largest corporations admit discriminating against veterans with general discharges, even though the Defense Department asserts that these discharges are "under honorable conditions."

Over 90 percent of the large corporations require veterans to submit a copy of their DD–214—discharge papers—when applying for a job. And 20 percent admit they have lists to decode the SPN's while others indicated that they would like to have the lists, which the Defense Department classifies as "official use only." There is no telling what happens to SPN information once it gets into the private sector. It may work its way into data banks to which hundreds of private users have common access. The General Accounting Office is now investigatiing the possibility of such abuse.

On March 22, Armed Services Committee Chairman F. Edward Hébert announced that the Defense Department was discontinuing its policy of placing SPN-type information on the DD–214 received by every serviceman when he is discharged. Under the new policy, however, SPN's would be assigned to the serviceman upon his discharge, but they would not appear on the DD–214. In addition, the new policy appears to permit the release of SPN-related information to private employers upon the request of the veteran.

The Defense Department's new policy has not yet been finalized in the form of regulations. When regulations are issued, there is a substantial likelihood that private employers will require veterans to request release of the information as a precondition to any job decision. While 20 percent of the large corporations admit having lists to decode SPN's many more may try to obtain information which would be available. The new policy could encourage private corporations to pressure the veteran to request release of the SPN-related information. In many cases such information is irrelevant to future job performance. But whether or not it is relevant, such an invasion of privacy cannot be justified or tolerated.

Mr. Speaker, I have just received answers from the Defense Department to a series of questions which I sent them earlier this year on the subjects of SPN's and types of discharges.

The Defense Department's letter speaks for itself, indicating quite clearly that DOD feels no moral or legal responsibility for veterans with unfavorable types of discharges or those with adverse SPN's.

Especially disturbing are the DOD answers to questions 9 and 17. The Defense Department states that the standard of proof required to award an adverse SPN is "that which is sufficient to persuade the recommending commander and the discharge authority that the reason for discharge and the character of service is warranted and appropriate." DOD states further that the standard of proof for awarding a general or undesirable discharge "is not determined by reference to issuance of either a general or undesirable discharge. Rather, the standard of proof is based on the reason for discharge." Perhaps the imprecise standards help explain why so few veterans are able to change their types of discharges or SPN's. I cannot believe that these standards of proof are not violative of constitutional due process of law.

I am also very disturbed by the Department's inclusion in its list of reasons for the rise in the rate of unfavorable discharges the "necessity to identify and discharge members who do not meet retention standards, especially during times of reduction of forces." Are we to accept higher rates of adverse discharges because the Defense Department is reducing forces? Why does the Defense Department feel it must brand servicemen as unsatisfactory in order to meet new force levels?

I was also interested in the answer to question 26, where DOD states that it is unaware of any studies supporting or rejecting the notion that the type of discharge is generally a good predictor of future civilian job performance.

Mr. Speaker, I do not know what the answers to all of the questions would have been before the change in SPN policy. I do know that the answers now furnished paint a picture of a Defense Department unconcerned with what happens to veterans with unfavorable types of discharges and adverse SPN's. I am somewhat surprised at the lack of regard for the rights of servicemen about to be discharged, who may forever be branded because of the Defense Department's disregard for their privacy.

I think that the Defense Department has a moral and a legal obligation to respect the privacy of servicemen and veterans. I have asked the Secretary of Defense to prohibit the disclosure of SPN information to private employers, even if the veteran requests the release of that information.

Armed Services Committee chairman said in announcing the new policy:

"The nature of the discharge should speak for itself, and that should be it as far as the discharge papers handed to the veteran are concerned. It is tough enough for a veterans with an honorable type discharge to become gainfully employed these days without carrying the additional burden of something that may not be relevant to a particular job as a civilian."

I agree.

Mr. Speaker, so that the Members and the public may have a better understanding of the Defense Department's policy on SPN's and types of discharges, I will tomorrow ask unanimous consent that the Defense Department's answer to my letter appear in the Record.

BANK SECRECY

Mr. STARK. Mr. Speaker, as author of the Right to Financial Privacy Act of 1973, a bill cosponsored by 102 of my colleagues, I am pleased to add to the discussion today on this most pressing issue.

I was also a plaintiff in a case on the constitutionality of the Bank Secrecy Act that this bill would amend, and the Supreme Court yesterday handed down its long-awaited decision. The Court in effect chose to skirt the issue by finding that the plaintiffs didn't have standing—and thereby threw the issue back into the lap of Congress where it was first created.

The Congress passed the Bank Secrecy Act in 1970 with the intention of assisting the war on crime. Its purpose was to facilitate the gathering of information on suspected criminals by permitting any Government official to have access to individual bank records. In addition, banks were required to report "unusual" currency transactions to the Secretary of the Treasury as well as all domestic transactions over $10,000. The banks, then, were to act as investigators for the Government—to spy on their own customers.

I filed suit with the ACLU and the California Bankers Association and got an injunction against those reporting provisions of the act. However since the record-keeping requirements were upheld, we appealed the decision, as did the Government from the other side, and it was thus cross-appealed up to the Supreme Court.

The Court's decision, therefore, was in a sense disappointing. However, in not addresing the constitutional issues, they left the way open for legislative remedy. And in fact, the dissenting opinions of Justices Douglas, Marshall, and Brennan and the concurring views of Powell and Blackmun can be interpreted as urging legislative relief to a problem that was caused by legislation.

I am hopeful that the Banking Committee, of which I am a member, will soon hold hearings on the Financial Privacy Act. If we act promptly it will be possible to pass this momentous legislation before the end of the session.

As my colleagues are well aware, this is perhaps one of the most critical issues of the time. Even the President has expressed a new-found concern for the safeguard of privacy and legitimized it by creating Gerald Ford's Commission on Privacy. Clearly then, this is the time to pass the necessary legislation. We cannot let this momentum pass us by.

For the interest of my colleagues, I would like to include in the Record some excerpts from a statement I made last summer on the Financial Privacy Act and some of my own experiences with abuses of confidence.

[The information follows:]

EXCERPTS FROM A STATEMENT BY MR. STARK ON THE FINANCIAL PRIVACY ACT

The bill I have introduced, H.R. 9424, resolves all the ambiguities in existing law relating to an individual's financial records. It clearly safeguards the individual's right to privacy with respect to his financial transactions and history. Specifically, the Right to Financial Privacy Act establishes four means of access to private records held by financial institutions: customer consent, administrative subpenas and summonses, search warrants, and judicial subpenas. Correspondingly, the act places an obligation on the financial institutions not to disclose information from customer records unless one of the above requirements has been met. In addition, it is stipulated that the information obtained by the Government must be used only for those purposes for which it was originally solicited.

The need for this act, while not resulting directly from the Bank Secrecy Act, stems from subsequent controversy over the precise interpretation of an individual's fourth amendment rights. At Senate hearings held last year on legislation to amend the recordkeeping laws, the Secretary of the Treasury admitted that subpenas are not required for the release of financial information. He suggested that as the 1970 act had not specifically addressed the matter of access to records, the Treasury could not take arbitrary administrative action to do so. It was therefore up to a bank to determine whether or not a subpena was necessary before records would be provided without the consent of the customer. The Treasury would take no position to supersede the bank's judgment.

In this situation, the privacy of a customer's financial records is dependent on the whim of his bank. Without his knowledge or consent, his entire financial history may be divulged. As he is unaware of official scrutiny, he cannot possibly challenge the dissemination of the information. There are no safeguards to protect this confidentiality.

In June 1972, I filed suit with the northern California ACLU and the California Bankers Association to test the constitutionality of this reporting system. The suit, asking for an injunction of the Bank Secrecy Act on the grounds that it authorized illegal search and seizure, was later joined by the Wells Fargo Bank. Bank of America representative Robert Fabian publicly voiced his own similar objections to the dangers inherent in the reporting provisions of the Act. He declared that "the regulations could undermine people's confidence in the banking system and the Government."

A Federal judge in San Francisco issued a temporary restraining order to prevent the act from taking effect. Subsequent to an appeals court decision, the Supreme Court is now deciding whether or not to hear the case.

This bill that I have introduced is not inconsistent with the essence of the Bank Secrecy Act. It recognizes the critical need for a thorough system of recordkeeping and reporting and upholds the requirements for reporting of information, subject to the previously mentioned limitations. Finally, the bill explicitly limits to two situations the Secretary of the Treasury's ability to require an institution to transmit reports or to keep records on customers. Such reports must either be required by the Internal Revenue Code, or by a supervisory agency. This, then, effectively repeals contrary provisions of titles I and II of the Bank Secrecy Act. However, I do not believe that their deletion in any way weakens the Bank Secrecy Act, or undermines its intent. Instead I believe it can only strengthen it, by removing any lingering doubt over possible or potential unconstitutional applications of its provisions.

This bill has already stimulated discussion. In particular, two areas of doubt have been raised, and I would like to attempt to answer them at this time. The

first is criticism raised by certain members of the law enforcement sector—that the limits placed on the Secretary's right to obtain reports will inhibit important criminal investigation. I believe that the legal processes still open to any law enforcement officer under this Act are sufficient. This act simply guarantees that customers be notified and have an opportunity to respond to any attempt to gain access to their records except where the standard of probable cause has been met. Within the bounds of the fourth amendment rights, that is all that is constitutionally possible.

Others have objected to consideration of this act at this time on the grounds that airing of the issue may bias the upcoming decision of the Supreme Court to review the appeals case. It must be remembered, however, that legislative action will take precedence over court action in such a way as to render that appeal inoperative. If passed, this act answers all the charges filed in the original California suit.

I would like to include for the information of my colleagues an excerpt from a supporting statement by the California Bankers Association. On July 19, the Association wrote that:

We should make it clear that, although the Association places a high value on maintaining the financial confidentiality which bank customers have come to expect, it certainly does not wish to deny it any way the necessary prerequisites of effective law enforcement. The Association feels, however, that it owes its highest responsibility to the banking public who have entrusted some of their most personal records of private financial affairs to our care. The public expects these records to be held in the highest confidence and the California Bankers Association welcomes legislation which would safeguard their expectations.

Mr. FRASER. Mr. Speaker, privacy is a basic right. But the growing network of information-gathering activities is threatening our constitutional right to privacy and individual freedom.

The law offers the individual protection against physical surveillance, but virtually none against data surveillance.

Computers make the vast collection of data on individuals collected by Government and private sources a danger to all residents of our country. This private information often includes highly personal, unverified hearsay and gossip. Illegal or even legal access to this data and the exchange and selling of such information without the knowledge of the individual involved endangers the basic right to privacy.

A person who voluntarily fills out a form, takes a psychological test, or has a physical examination may not consider or anticipate that confidential information resulting from these acts may well wind up in a computer and follow him for the rest of his life, affecting the course of his life.

One of the more startling examples of Government invasion of privacy was the Executive order—now fortunately rescinded—which gave the Department of Agriculture the power to inspect Federal tax returns of farmers "needed for statistical purposes."

We are all affected by the indiscriminate use of data collected—through credit records that often contain misinformation or computer mistakes; through health record data banks used by life, health and accident insurance companies; through bank records, military records, school records, and juvenile records. There is even a Government controlled data bank of information on children of migrant farmworkers. Intelligence gathering operations are carried out by some 20 Federal agencies and by State, county, and city agencies. There are many more examples of data collecting mechanisms such as airline computers, television surveys, psychiatric reports, and polygraph tests.

Recordkeeping may appear harmless on the surface. But we must have safeguards that will protect against the dangers inherent in this massive collection system.

Data surveillance is a chilling specter, intimidating and demoralizing.

I am committed to legislation that will guard against unwarranted access to such data.

Mr. MOSS. Mr. Speaker, we are frequently asked whose privacy is being invaded and how. What follows are a number of stark and freightening examples demonstrating how some law enforcement organizations and businesses have intimidated individual citizens. Hopefully these examples will serve to reenforce our commitment to the basic right of privacy for every American, for when one citizen's right is abused, all Americans suffer.

[The information follows:]

INDIVIDUALS VICTIMIZED BY INVASION OF PRIVACY

The $100,000 punitive damage suit of James C. Millstone against O'Hanion Reports, a New York-based retail credit reporting firm, goes to trial Feb. 19 in federal court in the eastern district of Missouri (72–C224–4). Millstone, assistand managing editor of the St. Louis Post-Dispatch and, incidentally, a member of the White House enemies list, is a classic unfair credit reports victim. He was turned down for auto insurance in 1971 because O'Hanion reported that "a poll of four neighbors proved" Millstone had a "lack of judgment," undisciplined kids, a prior history of evictions and a bad "attitude." Millstone received insurance coverage elsewhere but under the current Fair Credit Reporting Act, could receive only a verbal account, not a copy of his credit reports from O'Hanion. He then had difficulty getting the firm to correct its report, which proved to contain inaccurate allegations from one disgruntled neighbor in Washington, D.C.

A Princeton University faculty member, Galen L. Cranz, has filed a similar suit, wtih the aid of the ACLU of New Jersey, in federal court in Trenton (CA 1858–73). She was denied auto insurance on the basis of a Retail Credit Co. of Georgia report that mentioned that she was living with a man to whom she was not married. A Minneapolis woman suffered the same fate ("immoral behavior" according to the Safeco Insurance Co. and Service Review Inc.) but the state insurance commissioner may reverse the insurance cancellation as arbitrary.

A young couple were returning home to San Francisco one evening a year ago when they were stopped by Santa Clara County sheriff's deputies, eventually handcuffed, held at gunpoint and locked up overnight on charges of auto theft. The arresting officer had queried the San Francisco city and county criminal justice data bank and learned that the couple's Falcon had been reported stolen a year earlier. Police had failed to enter into the computer the "pink slip" record that the car had been recovered by its rightful owners. Eighteen hours after arrest, the pregnant woman and her husband were released. They have filed a $250,000 suit against Bay Area law enforcement agencies. "Not an isolated instance," according to their attorney, Bruce Krell of San Francisco.

It is in California where a San Francisco police cadet was fired for stopping a polygraph test about his sexual preferences and activities.

Arrest Records.—When Brad Shipp was named to the Fairfax County Board of Education in Virginia, it seemed like a great triumph for a 17-year-old high school senior. But the distinction turned promptly into a possible nightmare when members of the Board of Supervisors insisted upon seeing Shipp's arrest record after he revealed two arrests for the possession of marijuana. Virginia law forbids dissemination of juvenile records without the permission of the juvenile or the court. Shipp was saved when the Board deadlocked 4–4 and failed to reach the necessary majority to pass a motion asking Juvenile Court for Shipp's records. He is now serving as a member of the school board.

Arrest Records.—After Charles A. Tosh, an organizer for the Retail Clerk's Union, and others were arrested at a labor demonstration at a Buddies Supermarket in Fort Worth, the security director for the market tried to get the arrest records and mug shots of those arrested. First he tried asking his brother, the Dallas police chief, but was turned down. Then he called a buddy on the Fort Worth police force. This time he was successful, and the Buddies Supermarket displayed mug shots and "rap sheets" of the union organizers so that employees would be discouraged from voting for union representation.

When Tosh saw the anti-union posters, he hit the roof. The company was displaying the photo and arrest record of Charles Tosch, no relation to Tosh the organizer. Tosch was a convicted felon; Tosh had been arrested on minor charges and released.

The Fifth Circuit of Appeals (72–3017, June 22, 1973) held that the Fort Worth policeman's release of arrest records did not constitute "state action" and that Tosh's right to privacy was not violated by the company or the police. Tosh's lawsuit did succeed in showing that the Fort Worth policemen, like others around the country, make any of their 40,000 arrest records available to private security officers, as well as to other law enforcement agencies.

Arrest Records.—An enthusiastic 17-year-old youth was arrested at a rock concert in Columbia, Md., last fall and accused by a private security guard of throwing a rock. He denied the charge. The guard later disappeared, and so the charge was dropped and the youth's criminal file destroyed. However, the reference card to the charge remains in Howard County juvenile files and the young man is attempting to have it purged. "This could plague him the rest of his life," said his father.

Purging.—Among the 16 counts on which Baltimore State's Attorney Samuel A. Green was found guilty this month was a charge of accepting a $750 bribe to expunge the record of a Maryland man obsessed with the idea of having an arrest record (a 1971 gambling charge that was dropped because the man had no knowledge of the operation).

A U.S. District Court in San Diego last November refused damages for a woman ordered to undergo a strip search by border guards who noticed Chicano activist literature in her car. Nothing illegal was found. A $13 million suit has been filed against Macy's by seven employees who claim the firm illegally tapped their phones in the San Francisco store for seven months.

Mr. BADILLO. Mr. Speaker, I am peased to join my colleagues in this special order to signal a congressional commitment to privacy.

The age of technology has brought with it a flood of data banks, credit reference bureaus, computer lists, and government records with personal information on virtually every living American including allegations and rumors about spending habits, job histories, driving records, relationships with neighbors and fellow workers, academic performance, and even personality quirks. These and a host of other specifics are gleaned both from records filled out by the subject and from clandestine interviews with informants who are not necessarily well-informed about the subject but eager to volunteer what they know anyway.

The American people are entitled to be concerned about the big brother aspects of having the details of their private lives available on computer printouts for whoever has statutory authority or perhaps just the right connections to scan them. Evidence is available to us right now concerning unwarranted intrusion into the individual's constitutional right to privacy, and we in the Congress will have to take a stronger role in regulating, or even eliminating, some of the uncontrolled reporting and recordkeeping practices both among private entrepreneurs and agencies at all levels of government.

We have been given clear evidence that the credit ratings which affect a person's very reputation are often compiled on the flimsiest of information, sometimes exaggerated or falsified because of the financial premiums for investigators who submit unfavorable reports on individuals. Anyone who has ever been questioned about an acquaintance by Federal Government investigators is aware of the opportunity for malicious reporting and the deposit of unverified raw data into Government files that may remain observable by certain authorities for the duration of the subject's lifetime.

Because of the potential for abuse, and in fact because of increasing reports of actual abuses in the gathering and recording of private data on individuals, I am pleased that the Congress appears ready to move toward protecting the personal rights of the American people.

Mr. Speaker, I have cosponsored bills to require Government agencies to advise citizens what records are kept concerning them, to limit the sale or distribution of mailing lists by Federal agencies, to restrict the authority of Federal agencies to inspect individual income tax returns, and to guard personal privacy by regulating automatically processed files.

One of the greatest risks to our civil liberties now and in the future is the invasion of our personal lives through computerized data banks, wiretapping, and interception of correspondence. In anticipating the threat and acting quickly, we can put permanent limits on the snooping and secret information-gathering whose results accumulate in private and Government dossiers.

The pirvacy of the individual is one of our most cherished tenets. We have the opportunity to shore up and give real meaning to that important freedom. The legislation introduced by the Members participating in this special order should be among our highest priorities for the remainder of the 93d Congress.

Mr. ROSENTHAL. Mr. Speaker, the promise that each individual will be free from governmental surveillance of his or her political beliefs and activities is perhaps the most fundamental guarantee in the Bill of Rights, yet we find that his guarantee is increasingly being abused.

In the last decade there has been a vast increase in the maintenance and dissemination of all kinds of personal records by governments. These records contain personal information about virtually every aspect of the private lives of American citizens—from political dossiers to bank and credit records.

The dimensions of the dossier problem are already staggering and are steadily growing. For example, there are approximately 2,500 credit bureaus in the country with records on more than 131 million persons, all of which are regularly sold and disseminated. The Defense Department and the FBI compiled between 1968 and 1972 in the area of political surveillance a computerized index of more than 25 million names of persons who had taken part in civil rights or antiwar activities and were regarded as potential civil disturbance risks.

The profound danger of these files is that the individual may be totally unaware of the existence of these records and totally unaware of the contents. The impact and the existence of them may only become known in extraordinary circumstances. Yet the effect of the contents of the file may be earth shaking upon disclosure to employers, creditors, banks, or other agencies.

Often these dossiers create assumptions about people on the basis of anecdotal information about their past, and then condition the future of their lives on those frequently false assumptions. The individual seeking employment may suddenly find that a dossier has been compiled, containing false or erroneous information, that may eliminate him from contention for a job. For instance, the Federal Civil Service Commission has files on 1.5 million persons suspected of "subversive activities" and therefore, blacklisted for employment.

The subject of privacy has been studied extensively by congressional committees and subcommittes and by prestigious governmental and private agencies. It is now time for substantive legislative and administrative action to be taken to protect the right to privacy.

Several steps must now be taken to curb the antidemocratic tendencies of dossier-building. First of all, control must be established over data collection and computerized data banks maintained both by private and government agencies. Prohibitions must be established against the gathering and storing of information relating to the lawful political activities of individuals. Perhaps most importantly, every person about whom personal data is stored should be notified of that fact and given access to his dossier to check its accuracy and propriety.

I wish to direct your attention to an article "Your Past Maybe a Prison" by John H. F. Shattuck which dramatically highlights the importance and th eneed for legislation in this area. Only strong and prompt action to safeguard the right of privacy will convince the nation's citizens of the sincerity of their legislators and leaders in protecting individual privacy.

[Mr. Shattuck's article follows:]

[From the National Council of Jewish Women, October 1973]

Your Past May Be a Prison

(By John H. F. Shattuck)

About two years ago Robert Meisner received a letter informing him that his car insurance was being canceled because of an adverse credit report prepared by a nationwide commercial credit reporting agency. Never having had credit problems before, Mr. Meisner managed to find out, after a series of angry letters and telephone calls to his insurance company, that the report indicated his son was "a long-haired hippie suspected of drug use." The source of the report was never disclosed to Mr. Meisner. Since his son had no police record of any kind and was characterized as a model student by his high school principal, the insurance company eventually reinstated the Meisners' insurance in order to minimize the bad publicity resulting from Mr. Meisner's tenacity. Retail Credit Company, which had prepared the report, however, refused to expunge the erroneous and damaging information in the Meisner dossier—one of more than 50 million in its files—and it could not be compelled to do so under any existing law.

The Meisner case is symptomatic of the problems of a dossier society. Governmental and private activity to counter perceived threats of crime and subversion is a growth industry. The heart of this activity is record keeping. In the last decade there has been a vast increase in the maintenance and dissemination of all kinds of personal records—computerized records of arrests not resulting in convictions, political dossiers on private citizens who exercise their rights of free speech and assembly, medical and welfare records of persons who qualify for government assistance, bank records of private depositors in federally insured banks, credit records like the one that caused trouble for Robert Meisner, and a seemingy endless variety of other kinds of personal information about virtually every aspect of the private lives of American citizens.

These data collection and dissemination practices tend to trap those who get caught by them in a "record prison." It is difficult for a person to escape the effects of his increasingly bulky "record" because allegations of past misdeeds and judgments about him follow him whenever he seeks a job, a license, credit, housing, admission to school, or a host of other social benefits.

One ACLU client, for example, a former Post Office employee, was forced to resign when he was placed under investigation for mailing obscene letters. He was subsequently cleared of the charge but the Post Office refused to reinstate him and agreed only to make a notation in his federal Civil Service file that he had been cleared. Several years later, the man was disqualified for state employment by the Utah Civil Service Commission, on the basis of a file check which turned up evidence of prior "immoral conduct." Apparently the clearance notation had not been computerized with the rest of the man's employment record.

The major evils of these anecdotal records are their persistence and increasingly wide exchange. Bank records, for example, provide a detailed account of a person's political contributions and membership in private clubs or other organizations. By federal statute enacted in 1970 the Secretary of the Treasury is now empowered to require banks to microfilm and maintain for periods up to five years all checking transactions, and to make reports about such transactions to the Secretary, who, in turn, can make them available to other government agencies. All these financial records, therefore, are available to the government without any notice to the depositors, whose privacy and rights to political anonymity are quietly subverted.

In terms of the sheer quantity of available data of private persons, the dimensions of the dossier problem are staggering. There are, for example, approximately 2,500 credit bureaus in the country with records on more than 131 million persons, all of which are regularly sold and disseminated. Of the more than 7.5 million arrests which are recorded each year, 3.5 million do not result in convictions but continue to be recorded and widely disseminated for a variety of purposes, including employment screening. A 1967 study of employment agencies in the New York area indicated that 75 percent would not accept for referral an applicant with an arrest record and no conviction.

A similar study by the U.S. Employment Service in Washington revealed that only about 15 percent of job applicants with records of convictions or arrests could be placed. In the area of political surveillance, the Defense Department and the FBI between 1968 and 1972 compiled a computerized index of more than 25 million names of persons who had taken part in civil rights or antiwar activities and were regarded as potential civil disturbance risks. The federal Civil Service Commission has files on 1.5 million persons suspected of "subversive activities" and therefore blacklisted for employment. Moreover, those examples are only the tip of the iceberg.

Some of the least dramatic records can have the most profound impact, but are never known to their subjects, or only become known in extraordinary circumstances. Mark Isaacs is a professor at Temple University. Three years ago his eight-year-old son David was killed in a highway accident, and during the course of litigation, David's school records were obtained by the lawyers. When Mark Isaacs read these records his outrage at what they contained prompted him to write an article, "The Secret File of David Isaacs, Age 8," which was published in the Philadelphia Inquirer. One anonymous comment in the file stated, "Refuses to use left hand. Dislikes being reminded to try." David's father pointed out, "Of course he refused; of course he disliked nagging. He had an orthopedic problem on his left side . . ." In another part of the article Mark Isaacs indicated that "two months before he was killed, David was given a standard psychological test. . . . The comments appended by the school psychologist fascinate me. This time the comments are signed. 'Subject boy had bad associates,' the psychologist declared. 'The bad associates were his parents. . . . David's feelings of superiority, if they do exist, are bolstered through parent attitudes.' "

David Isaacs' school record represents all that is wrong with the dossier society. Data gathering and dissemination frequently work the way a tracking system works in a school; they create assumptions about people on the basis of anecdotal information about their past, and then conditions the future of their lives on those assumptions. For this reason these practices are often antithetical to a free and open society which allows people the opportunity to improve their lives.

Several things should be done to curb the antidemocratic tendencies of dossier-building. First, there should be a flat prohibition against gathering and storing information relating to the lawful political activities of individuals. Second, legislation outlawing the storage or dissemination of hearsay or anonymous derogatory information should be enacted. Third, procedures should be devised for expunging or preventing the dissemination of records of arrests which do not result in convictions. Fourth, we must evolve a procedure analogous to the eco-

nomic bankruptcy process whereby an individual can gain a "discharge" from his past. Just as the commercial process cannot function without a procedure enabling participants to attempt a fresh start, the social system cannot function without a procedure enabling individuals to obliterate the residue of their past errors. Finally, every person about whom personal data is stored should be notified of that fact and given access to his dossier to check its accuracy and propriety. Under a new federal statute, the Fair Credit Reporting Act, subjects of credit investigations must be notified that they are being investigated, but they have no right under the statute to see their reports. One way of starting this mammoth notification task would be to compile an exhaustive citizens' guide to files of personal information in the federal government.

A remedial program with these general features would begin to reduce the danger to freedom inherent in the dossier society. The alternative is to march bravely toward a new world in which privacy and freedom are replaced by suspicion and security, and the secret computer printout reigns supreme.

Mr. STEELMAN. Mr. Speaker, the congressional commitment to privacy must hard-hitting, immediate, and two-edged. For too long unjustified secrecy and privacy have proliferated throughout government, and for too long the government has, in the name of efficiency and law and order, and sometimes unintentionally, violated the citizens inherent right to privacy.

These two democratic rights, the right to know, and the right to privacy, have helped build that vital dimension of difference that sets America apart from most other nations of the world.

When the Freedom of Information Act was enacted in 1966 we were all confident that a new era of Government accessibility was being ushered in. But those of you who have tried, or have read about the unsuccessful and arduous processes involved, know that the Freedom of Information Act does not always work. There is still too much information being withheld, and there is still too much delay in responding to requests for information. There is no persuasive logic, certainly no commitment to democratic principle, in those arguments, that claim that without secrecy and covertness, modern and efficient government cannot function. Are we not, by such arguments, trying to preserve our democracy, by methods that by their very nature threaten its health and well being.

These matters are serious, and that is why I am working on legislation that will amend title 5 of the United States Code, to make freedom of information a fact, and not just an act.

But as my honorable colleague from California has emphasized, the right to know is only half the issue, the right of privacy is its necessary complement. With the increase in the use of the social security number as a standard universal identifier, and the indiscriminate and uncontrolled assimilation of personal information into hundreds of data banks, there is a grave threat that national dossiers will become a fact. At best, this is a frustrating and annoying invasion of privacy, and at worst, it may threaten a denial of status and benefits without due process of law.

I ask that we create an alliance of commitment to insure that our right to privacy, and the right to know are not empty words, but strong, powerful realities.

Mr. HEINZ. Mr. Speaker, I express my thanks to my colleagues Mr. Horton and Mr. Goldwater for giving the Members of the House this opportunity to express our commitment to privacy.

One natural outgrowth of an increasingly technological society is the dangerous proliferation of computerized personal records on every individual. Such devices, while perhaps well intentioned, deprive people of the privacy that should be their right. In addition, while it is quite easy for incorrect or misleading information to creep into one's file, once there it is considerably more difficult to get it removed. To cite some examples:

Last year a professor's wife in Texas lost her auto insurance because her credit bureau listed her as an alcoholic. She never drinks.

In New York a young woman has been fighting a Civil Service Commission order that she be fired from her job as a substitute postal clerk. It had been learned from her FBI computerized file that while a student, the woman, exercising her first amendment rights had taken part in a campus demonstration while at Northwestern University, and that she had been a member of SDS, a legally constituted organization.

In Massachusetts last year Gov. Francis Sargent had given a full pardon to a former felon who had kept his record clean for 10 years. He moved to a State 1,000 miles away and enrolled at a community college. However, after running

a routine police check with the new State's computer file and having learned of the man's past conviction, the president of the college expelled him. The listing did not include the full pardon. Even after Massachusetts officials had verified the facts of the case, the president refused to readmit the man to the school.

There have even been cases of employees stealing computer files on magnetic tape and using such information for their own purposes.

Whether it be protection from unfair credit reports, from unwanted pornographic materials, from needless harassment by junk mail, or protection against unfair discrimination based on one's background, each citizen has a right to expect that the government will take whatever action is necessary to insure individual privacy. This trend toward centralization of personal information at the expense of individual rights must be stopped!

On January 3, 1973, I introduced legislation, H.R. 632, that in my opinion, goes a long way toward protecting individuals against invasions of privacy. This bill would prohibit the sale or distribution of mailing lists and other information without the consent of those people whose names appear on the list. Other bills concerned with privacy are also pending before the Congress, and I hope that strong action will soon be taken. Clearly, it is long overdue.

An employee of the Book-of-the-Month-Club—membership 1.5 million—reports:

"The saddest thing of all is reading letters that begin, 'Dear Computer, I know there are no humans there.'"

I urge this Congress—with action as well as with words—to go on record as being determined to help make this society a little more human, and a little less machine. People must come first. It is up to us to see that they do.

Mr. RANGEL. Mr Speaker, the steady and uncontrolled invasion into the private lives of American citizens must not continue unchecked by Congress. The use of information obtained for one purpose which subsequently becomes part of a data bank for entirely different purposes is a process we must closely watch and tightly control.

I would like to submit the following article which identifies a potentially dangerous invasion into the privacy of American citizens in methadone programs in the Washington, D.C., area.

[The article follows:]

[From the Washington Star-News, Oct. 28, 1973]

FOOTPRINTS "IDENTIFY" METHADONE PATIENTS

(By Lawrence Feinberg)

Under a sign of a large green foot, Washington's narcotic treatment administration has collected about 5,000 footprints during the past two years in an effort to keep track of the methadone it dispenses.

"They laughed at us when we started," recalled Ronald J. Nolfi, who heads the agency's footprint project. "What's a footprint? But now they see it works."

The agency promises to keep the names of the heroin addicts it treats confidential. But Nolfi said it also needs a way to make sure that the same person using more than one clinic to collect methadone, an addictive, inexpensive heroin substitute.

"A lot of people have a lot of emotional problems about giving fingerprints," said Dr. William Washington, NTA's acting director, "even though we assure them they won't go to the police."

The solution, since early last year, has been to collect footprints, which like fingerprints, are different for every individual but which the FBI doesn't keep.

Nolfi and two assistants classify every footprint they take. They use the right foot only and file the prints by the large green foot which is really a bath towel. Their office also has a foot-shaped ashtray, and a foot-shaped note pad, called "Footsie Notes."

Each day the footprints of addicts signing up for treatment are checked in the files. If the same prints are there already, NTA counselors try to sort out the identity problem and make sure no one is getting more than one dose of methadone a day either to use themselves or sell illegally.

Since the footprinting started, Nolfi said, about 20 addicts have been caught trying to go to more than one clinic. About 250 others, he said, have been found trying to get back into the program after dropping out without telling that they had been in before.

Even though many hospitals take footprints of babies to make sure they won't be mixed up, Nolfi said nobody classified footprints and stored them until NTA set out to do so.

The system for classifying was worked out by the National Bureau of Standards. It uses the lines and swirls on the ball of the foot.

The patterns under the big toe are called the core area. They are divided into seven basic types. For patients that don't fit into a basic group, there is an eighth category called "accidental patterns."

The lines under the four smaller toes are called the secondary area, and they are divided into nine basic patterns.

To finish the classification the distance is measured in millimeters from the center of the core area to the point where the lines diverge.

To do the classifying takes about a minute, said James Schmidlin, a technician at the NTA center at 20 H St. NE. To search the files takes about 10 minutes more.

There are no names in the files to make sure they are confidential, just code numbers, which are matched elsewhere. But on the back of each footprint card there is basic information about the patient, his drug habit and treatment.

Schmidlin said only one patient has refused to go through with the footprinting, and very few raise any objections.

One reason for the lack of fuss, he said, is that the files really are kept confidential. Another is that the footprinting is made part of the regular medical exam, and is quick and clean. It's not done with ink, but with a clear liquid which reacts with a chemical coated on the card without leaving any stains on the foot.

The cost of each print is about 15 cents, but overall the program has cost $50,000, provided by the Law Enforcement Assistance Administration.

Since this summer the five other programs dispensing methadone in the Washington area also have been taking footprints of their patients and checking them against the NTA files.

The White House Special Action Office on Drug Abuse prevention is trying to have footprint files by drug treatment programs elsewhere in the country, but so far no one outside the Washington area is doing it.

Mr. MYERS. Mr. Speaker, resolving the issues related to right to privacy requires expert assistance. I am pleased that the National Bureau of Standards, Institute for Computer Sciences and Technology has taken privacy and security in computer systems as a main focus of their mission. Two conferences have been sponsored by the Institute bringing together several hundred computer specialists and information users in the Federal and State scene and the private sector.

By way of introduction to defining and reestablishing privacy rights, Dr. Ruth Davis led a group of speakers who described the nature and scope of these problems.

I believe this summary of their presentations would be of value to my colleagues and include herein.

[The summary follows:]

PRIVACY AND SECURITY IN COMPUTER SYSTEMS

There is a tendency to confuse the issues of privacy, confidentiality and security with respect to recordkeeping and computers. Dr. Ruth Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards, outlined the essential differences between these issues and established a framework for unambiguous discussion and solution of these problems.

Privacy is a concept which applies to *individuals*. In essence, it defines the degree to which an individual wishes to interact with his social environment and manifests itself in the willingness with which an individual will share information about himself with others. This concept conflicts with the trend toward collecting and storing personal information in support of social programs of various importance. The government's role often makes the supplying of this information mandatory—thus, creating a direct and acute compromise of the individual's privacy. Under this circumstance, the burden of protecting personal data is all the more important.

Confidentiality is a concept that applies to data. It describes the status accorded to data and the degree of protection that must be provided for it. It is the protection of data confidentiality that is one of the objects of *Security*. Data confidentiality applies not only to data about individuals but to any proprietary or sensitive data that must be treated in confidence.

Security is the realization of protection for the data, the mechanisms and resources used in processing data, and the security mechanism(s) themselves. *Data Security* is the protection of data against accidental or unauthorized destruction, modification or disclosure using both physical security measures and controlled accessibility techniques. *Physical Security* is the protection of all computer facilities against all physical threats (e.g., damage or loss from accident, theft, malicious action, fire and other environmental hazards). Physical security techniques involve the use of locks, badges (for personnel identification), guards, personnel security clearances and administrative measures to control the ability and means to approach, communicate with, or otherwise make use of, any material or component of a data processing system. *Controlled Accessibility* is the term applied to the protection provided to data and computational resources by hardware and software mechanisms of the computer itself.

From these definitions, it is possible to see that there is no *direct* relationship between privacy (a desire by individuals, groups or organizations to control the collection, use or dissemination of information about them) and security (the realization of the protection of resources), although they are interrelated. Several speakers pointed out that a perfectly secure computer could be used in such a way as to violate individual privacy. However, this should not be construed as an excuse for not creating secure computer systems since the thrust of earlier remarks was to the effect that legislatively defined rules for assuring privacy are now levying a security-oriented environment on government (and possibly private) data systems.

2.3 SOCIAL IMPLICATIONS

Dr. James Rule, Professor of Sociology, State University of New York at Stony Brook, presented a sociologist's view of the privacy question. He observed that the issues of privacy are social-political-human rather than technological and that the question of how far to go in computer-based recordkeeping on people is a political/social question in which the rights/needs/interests of the individual must be weighted against the rights/needs/interests of "institutions (social, political, commercial, etc.). In his view, determining the proper balance between individual privacy and institutional needs and interests will involve even more agonizing choices in the future than it does now. To illustrate his point, he described a hypothetical situation revolving around the use of computerized recordkeeping control of crime. In the hypothetical (but potentially feasible) situation, statistical methods of behavior analysis are used to predict individual criminality before it occurs. Assuming that such a system could be assured of evenhanded administration, would such a system be desirable and would it justify the extensive recordkeeping on *all* individuals necessary to make it work?

2.4 LEGISLATIVE ACTIONS

As a result of the early warnings and studies of the privacy issue that have taken place in this country over the past 7–8 years, a number of legislative actions have taken place or are contemplated. For example, three Federal Acts have been passed in recent years relating to the issue of privacy. These are the Freedom of Information Act, which provides for making information held by Federal agencies available to the public unless it comes within a category exempted by the Act; the Federal Reports Act, which establishes procedures for the collection of information by Federal agencies and the transfer of confidential information from one agency to another; and the Fair Credit Reporting Act, which requires consumer credit reporting agencies to adopt procedures which are fair and equitable to the consumer with regard to confidentiality, accuracy, relevancy and proper use of such information. The Fair Credit Reporting Act also established the right of the individual to be informed of what information is maintained about him by a credit bureau or investigatory reporting agency.

In addition to these pieces of legislation, numerous bills have been introduced in Congress which propose to strengthen the rights of individuals with respect to confidentiality of data, prevent invasion of privacy, establish standards for the collection, maintenance and use of personal data, or limits the uses to which personal data can be put without written consent of the affected individual. It was also reported at the Conference that the Department of Health, Education, and Welfare (DHEW) is implementing (internally) the

recommendations contained in the Report of the Secretary's Advisory Committee on Automated Personal Data Systems.

The 50 State governments have pending numerous bills concerned with protection of individual privacy and data confidentiality. Massachusetts and Iowa have already passed significant legislation in these areas, providing higher standards of personal privacy protection than the Federal Government. Still other States have extensive legislative proposals that would impose extensive regulatory and technological constraints on the operation of personal data systems.

At the local level, a number of municipalities have passed ordinances to provide protection of computerized personal data.

While all of this legislative activity is not completed, it is indicative of the political response to the aforementioned public awareness and concern over individual rights and privacy.

2.5. THREATS

Threats to individual privacy and technological threats to computer-based information systems were the two themes repeatedly stressed by the various speakers. While the threat to individual privacy and liberty was predominant and seen to be mostly associated with the unregulated collection and use of personal data, a number of the speakers cited the technological threats as being those most bothersome to the operators of information systems.

Most of the speakers agreed that the threat to privacy was one that required legal and regulatory remedies and was not basically a technological problem. All speakers agreed, however, that technology was required to help enforce the legal and regulatory steps. Furtermore, a number of speakers noted that unless there were sound technological foundations for controlled access to computer systems, the legal and regulatory actions would be largely wasted.

In addition to the basic and somewhat diffused threat to individual privacy posed by the collection and use of personal data, several speakers cited an additional problem of misappropriation and misuse of data by people who are authorized access in connection with their jobs. While the problem of misuse of data would appear to be one solved by legal measures providing stiff penalties for violators, several speakers indicated that it was in part technological since the contemporary systems have so little in the way of controlled access mechanisms that it is difficult to restrict access *within* a data base and to account for its access and usage.

The degree of difficulty and the cost associated with providing security and controlled access to computer-based recordkeeping systems is a function of the type of access being permitted, the capabilities of those performing the access, and the type of computer system (whether dedicated, shared, local or remote access, etc.) on which the recordkeeping system is based.

Mr. HUDNUT. Mr. Speaker, today I am pleased to join my colleagues in a special order regarding the congressional commitment to privacy. I am glad to have the opportunity to express my personal concern for retaining and restoring this vital individual liberty in America.

In this computer age, it is easy to obtain information about an individual. Much concern has been voiced over the extent to which citizens' privacy is being invaded. We see this in the accumulation of personal data in computer banks and other such means which constitutes a threat to the privacy of every American citizen. There are some who look upon individual tax returns as the greatest source of such information.

The assurance provided the American people that information voluntarily given on Federal tax returns will be carefully protected from disclosure and improper use is one of the basic concepts underlying this country's system of collecting taxes and I want to assure that protection. I am cosponsoring legislation (H.R. 10977) which will further restrict accessibility to taxpayers' tax returns.

Even though the matter which precipitated this bill; namely, the move to check tax returns of farmers' ostensibly for the purpose of obtaining information on which to base farm programs, has been resolved, it is my hope that the Ways and Means Committee will grant early and favorable action so the authority for inspection of individual tax returns by Federal agencies will be severely restricted.

Mr. ASHBROOK. Mr. Speaker, during my seven terms in Congress I have been deeply concerned about the increasing centralization of power in the Federal Government and the tendency of that Government to intrude more and more

frequently into the personal lives of its citizens. I strongly believe that our citizens cannot afford any further erosion of their privacy.

Therefore, I was one of the first to urge the administration to revoke a controversial Executive order which allowed the Department of Agriculture to obtain personal financial information from the income tax returns of farmers. A little over a week ago my position was upheld and the President rescinded his order.

I have also moved to repeal legislation which allows the Secretary of Health, Education, and Welfare and officials under him to look at private medical records of people who receive medicare assistance. I believe that doctor-patient records are confidential and should not be given to Government officials.

These two incidents are part of the bigger issue of privacy for every American. At a time when technological progress is making it possible for the government to compile more and more information on all Americans, there is much room for misuse of the information collected.

Dr. Jerome B. Wiesner, president of the Massachusetts Institute of Technology, has warned in an article that—unless we act now to place safeguards on the "informational revolution"—George Orwell's "1984" could come to America. Without endorsing all of Dr. Wiesner's opinions or proposals, I do believe that his statement should be read as widely as possible. Therefore, I include the following excerpt from his article with my remarks.

[The excerpt follows:]

THE INFORMATION REVOLUTION—AND THE BILL OF RIGHTS

(By Jerome B. Wiesner)

The way in which we use and control the great new capabilities being created by the information revolution will shape the future character of our society; it may be said, indeed, to be shaping it already. Technology has been providing mankind with new tools and new opportunities for a long time and, in response, society has evolved new institutions and has changed its physical form. Sometimes these responses have been comfortable and swift, as in the case of the telephone and radio, at other times, they have been halting and painful, requiring repeated trials with many errors to find a new equilibrium that was comfortable for the society.

KNOWLEDGE IS POWER

For a long time, the rate of technological progress was sufficiently slow to enable society to adopt to the required change without permanent distortion of values. The pace of change is now very swift. We say "time is shorter now", and that is why we are faced with our present problem. To make the matter particularly urgent, information threatens to undo that subtle balance achieved in the Constitution between the people and the state which avoids anarchy on the one hand and tyranny on the other. Nowhere is it more true that "knowledge is power." Information technology puts vastly more power into the hands of government and the private interests that have the resources to use it. To the degree that the Constitution meant for the power to be in the hands of the "governed," the widespread collection of personal information poses a threat to the Constitution itself. There is also no doubt that technology can be and has been used to assist in the violation of the Bill of Rights. But it must be remembered that the violations are made by humans, not by machines. To my non-legal mind, there is even the question of whether the Bill of Rights, drafted in a simpler time, is adequate to protect man in his relation to the modern state and, whether there isn't a need for additional amendments providing protection for the individual against possible new infringements of his liberties.

Because many of our difficulties stem from the unforeseen side effects of technology or from the misuses of technological capabilities, there is a growing resentment and antagonism toward science and technology. There is also a widespread feeling that mankind would be better served if we could retreat to a simpler time. Given the present size of the world's population and the complexities of modern society, this hardly seems possible. In fact, I am firmly convinced that only through the sophisticated and careful use of technology can we create a truly decent society. In this circumstance, we must learn to manage technological change effectively for the common good. This, it seems to me, is the particularly important and urgent task of the Congress. Many

committtees of the Congress are concerned with aspects of this problem (such as the present hearings on the SST), but there is little focus on the overall task.

1984 COULD COME UNNOTICED

Modern information technology provides the potential to add to our general well-being and to enhance human freedom and dignity if properly used by extending our muscles, brainpower and material resources. Yet it also threatens to ensnarl us in a social system in which controls could essentially eliminate human freedom and individual privacy. Improperly exploited computer and communication technology could so markedly restrict the range of individual rights and initiatives that are the hallmark of a free society and the foundations of human dignity as to eliminate meaningful life as we appreciate it. In other words, 1984 could come to pass unnoticed while we applauded our technical achievements.

The great danger which must be recognized and counteracted is that such a depersonalizing state of affairs could occur without specific overt decisions, without high-level encouragement or support and totally independent of malicious intent. The great danger is that we could become "information bound", because each step in the development of an "information tyranny" appeared to be constructive and useful. I suspect that it would be much easier to guard against a malicious oppressor than to avoid being slowly but increasingly dominated by an information Frankenstein of our own creation. (Though we should recognize, I believe, that an effective means of citizen surveillance and intimidation could also provide attractive opportunities for a would-be dictator.)

CONTROL OF INFORMATION

Present and growing capabilities for surveillance and control are made possible by modern communication and computational techniques. It is very clear that such capabilities, through data-centralization and manipulation, will continue to grow at an ever increasing rate as our understandings of communications, computation and cognitive processes expand. At the same time, it is obvious that means for effective record keeping, information gathering, and data processing are essential needs of a modern society. The problem is to determine how to reap the maximum assistance from modern technology in running a better society and at the same time, how to keep it from dominating us.

In order to do this, we may have to adopt some stern measures in the form of very strict controls on who can do what with private information about any individual in the society. The present capabilities in information collection have already led to clear-cut infringements of citizens rights. In fact, even without technological assistance, there have been serious violations of the Constitutional protections by many agencies of the government and by many private organizations. Furthermore, the awareness of security dossiers has inhibited many people in their political activities.

WHAT KIND OF SOCIETY ARE WE BUILDING?

There is one specific point which I would like to stress. The issue of constitutional rights is but one dramatic aspect of the major problem of our time; namely: given so many options by a rapidly developing technological capability, what kind of a society are we going to allow to be created for ourselves and for our descendants? We live at a moment in history—I believe a unique moment—when the decisions we make, the paths we take, will shape the future of man's world for a long time to come. Technology allows us exciting opportunities for shaping a world to our liking, but it also poses the possibilities of a disastrous misstep. People everywhere have begun to appreciate that the thoughless applications of technology on a large sacle, done with the best of intentions and for the most constructive purposes, can frequently have large-scale destructive—at least, very unpleasant—side effects. We have slowly come to realize that we can intervene into the workings of the physical world on a scale and in ways that actually threaten man's survival on this planet. Fortunately there is a widespread reaction against such careless actions; witness the growing concern for the environment and the growing disenchantment with war, particularly nuclear war, as an instrument of foreign policy.

THE EFFECTS OF SMALL-SCALE VERSUS LARGE-SCALE APPLICATIONS

We are also beginning to understand that we can affect man's social and psychological environments in equally disturbing ways. We have learned one particularly important lesson about all of this. It is that technological innovations that are wholly constructive when employed on a small or moderate scale can, with increased and constant application, have such serious impact on the environment or on the society that massive efforts are required to offset their disastrous side effects. Sometimes a technical innovation can affect both the physical and psychological environments. The automobile, electric power and the aeroplane all illustrate this point.

The early manufacturers of automobiles hardly anticipated that their machines would produce the Los Angeles smog, the blight of our cities, or the malaise of the suburbs. And even today, the individual user of a bit of technology such as the automobile, a pesticide or a polluting detergent clearly believes that his personal gain greatly outweighs the environmental hazards that his small transgression produces. On the other hand, it is perfectly obvious that citizens of our country are sufficiently concerned about these problems to be willing to legislate against pollution even at the price of considerable inconvenience and cost. They are ready to spend substantial sums of money for less destructive products and large sums to undo the environmental damage from the past.

WEAPONS CONTROL

An important lesson can be learned too from our efforts to control weapons systems. It is much easier to stop the application of a specific piece of technology on a specific technique or a new strategy before it has been developed or widely applied, than after the fact. For example, it was relatively straightforward for the United States and the Soviet Union to agree to prohibit the introduction of nuclear weapons in outer space or on the ocean sea beds because these weapons did not exist. In contrast, it has proven impossible to curtail the emergence of anti-ballistic missile systems, even in the face of widespread agreement that they can't be effective, because they do exist and the decision to halt their development and deployment is contrary to the interests of large groups of people. It is perfectly obvious that this is a generally applicable theorem. If we want to avoid traumas from the mis-application of technology in the future, we should learn to recognize the inherent environmental or social threats in an early stage of a new technological development. I think that this point is particularly important in the matter of preserving privacy and freedom. The motto "eternal vigilance is the price of liberty" applies here with special meaning.

SURVEILLANCE OF PEOPLE

Modern electronic aids are not required for the operation of a comprehensive surveillance operation. In fact, the very effective security systems run by the Defense Department and the FBI during and after World War II made only modest use of electronic information storage and retrieval. But such systems were consequently quite expensive and also limited in the number of people that they could watch over closely. They frequently bogged down when presented with too much information. Large-scale data systems now operated by government bureaus and even private credit bureaus maintain files on tens of millions of people with no difficulty whatsoever. Furthermore, as you know, interconnecting communication networks allow information in separate files to be coordinated and centralized with great ease. In addition, as the software for data analysis becomes more sophisticated, it will be possible to simulate patterns of behavior for individuals and social groups and attempt to predict or anticipated their behavior with the purpose of maintaining better surveillance on individuals who, in one sense or another might represent a threat to someone having access to the data system.

TECHNICAL SAFEGUARDS ARE NOT ENOUGH

There are those who hope that new technology can redress these invasions of personal autonomy, existing or prospective, that information technology makes possible, but I don't share this hope. To be sure, it is possible and desirable to

provide technical safeguards against unauthorized access to data banks or information transmission systems.

It is even conceivable that computers could be programed to have their memories fade with time and to eliminate specific identity when the information was being processed to provide social profiles, etc., and such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal system of this country. We must face the need to provide adequate guarantees to individual privacy.

SPECIFIC NEEDS

I am a communications specialist, not a legal expert, and consequently, I hesitate to propose specific legislation. However, I have spent considerable time thinking about the issues involved and I would like to mention several specific needs which I see. These are:

(1) A watchdog authority, perhaps an independent agency, possibly a division of the General Accounting Office, perhaps the FCC, to review regularly the public and private information gathering and processing activities within the country. The agency should have the authority to examine the nature and extent of such activities and should report its findings to the Congress and the public.

(2) Congress should set rigid limitations on permissible surveillance activities and establish much stronger safeguards than now exist against misuse of data-file information.

(3) Action should be taken as quickly as is feasible to re-establish public confidence in the capacity of the boundaries of an individual's physical and psychological living space, his will require a number of steps. Outlawing some activities such as the free exchange of private information, collecting data not needed by an agency, etc., will help a good deal. Acknowledging publicly the extent of permissible surveillance and by whom is also important. Requiring disclosure of non-security type data to the concerned individual seems possible in many situations. In the few situations where this will not work, as in national securtiy matters, judicial controls should be strong.

(4) Technical means of insuring data security and safeguarding privacy should be developed vigorously and their use required.

A BALANCE BETWEEN THREATS TO FREEDOM—AND FREEDOM

We should be prepared to accept the cost of considerable inefficiency in our various social and governmental processes to safeguard our privacy and, as I judge it, our freedom, dignity, happiness and self-respect. By costs, I mean both the financial costs and the loss of a degree of control that the state might otherwise have over genuinely threatening individuals such as criminals and violent revolutionaries. Our task is to achieve a proper balance between the ability to cope with individual threats to the society and its capability to abridge the freedom and happiness of its members. In countries where the legal system cannot be counted on, the people are at the mercy of the administrator and they must hope that the bureaucracy will be benign. Such a situation smothers freedom. Because I believe that an "information tyranny" poses a very serious threat to the survival of a free society in our country, I vigorously recommend that Congress take whatever steps are necessary to bring the Bill of Rights up to date.

Mr. REGULA. Mr. Speaker, my colleagues, Messrs. Goldwater and Koch have my thanks for taking this special order to discuss the need for the establishment of a national privacy policy.

Examples of our need for such a policy are found in the everyday lives of all Americans, from the welfare mother to the corporate vice president: Eligibility regulations for food stamps and aid for dependent children; social security numbers for identification purposes; credit cards and credit data banks, a thriving business in consumer lists and personal information requested in census questionnaires, to name a few.

In this House alone there are 207 different sponsors of 102 different bills and resolutions relating to the protection of privacy. In April of last year, the House Government Operations Subcommittee on Foreign Operations and Government Information held hearings on Federal use and development of information techniques. Their findings and the evidence seems compelling that the Government must begin to pay more attention to the effect of its actions and the actions of the commercial world upon the rights and privileges of private citizens as guaranteed in the Bill of Rights.

The ramifications of data collected can and should be controlled in the first instance by the Federal Government's exercise of self control. Government data bank proposals should be studied to insure that data gathering is in furtherance of a purpose rather than self perpetuation. Data once collected should be reviewed and if no longer relevant, destroyed. Perhaps most important is the question of an individual's access to the records and data maintained about himself. One of the basic tenets of our system of law is the right to confront a witness or an accuser and to cross-examine him in order to elicit the truth. The written word or computer punch card bears witness as eloquently as the spoken word. The right of access to and challenges of data bank information by the subject of that information could, if exercised under the same or similar rules, only instill confidence in and aid our governmental processes.

An amendment which I cosponsored to the Freedom of Information Act that would increase public access to Government information passed the House on March 14. That bill would permit Federal courts to review Government information to decide if it should be released to the public and would give judges authority to require a prompt response to a citizen's request for information.

This is but a step in the right direction.

A serious evaluation of rules for data sharing and confidentiality should be made and boundaries should be drawn. Discretion is required in revealing data from one organization to another. In order to protect the privacy of the individual involved, he should have the opportunity to be informed of data sharing and offer his consent.

From Federal to State to local action, the question of privacy is involved. It is only through continued evaluation and new Government policies that we will really be capable of offering privacy to Americans in every realm of society.

Mr. ANDERSON of Illinois. Mr. Speaker, in 1933 in an address in New York City, George Bernard Shaw stated categorically that—

"An American has no sense of privacy. He does not know what it means. There is no such thing in the country."

In the more profound meaning of the word connoting the relationship between the citizen and his government, Shaw's words could not possibly be more misleading, because the Government of the United States was conceived and organized largely for the purpose of protecting the privacy of the citizen from unwarranted encroachments by his government and fellow citizens.

The first amendment prescribes that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof." No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in the manner prescribed by law," reads the second. The fourth amendment guarantees the right of the people "to be secure in their person, house papers and effects." The fifth amendment guarantees that the people shall not "be deprived of life, liberty or property, without due process of law." The ninth amendment, moreover, states that "the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

No less than 5 of the 10 Bill of Rights ratified in 1791 guarantee directly the sovereignty of the people in the pursuit of privacy in the broad sense. Indeed in each of the first 10 and subsequent amendments to the Constitution, the watchword is the protection of the citizen in the pursuit of his private interests from the unwarranted intrusion of the Government. In the past year when it has so forcefully been brought to our attention that men in the highest offices in the land have paid little more than lipservice to these principles, it might behoove each of us in the quiet and security of his own home to re-read the founding protections and principles legitimized by the Constitution.

I am reminded of an obseravtion made by Walter Lippman that—

"Those in high places are more than the administrators of government bureaucracies. They are more than the writers of laws. They are the custodians of the nation's ideals, of the beliefs, it cherishes, of its permanent hopes, of the faith which makes a nation out of a mere aggregate of individuals."

The 102 bills and resolutions presently pending before the committees of this body, sponsored by nearly half the Members of this body, are surely concrete examples that this body is intent upon protecting the ideal of privacy.

All of the body of law that has been developed in the nearly 200 years of this Nation's life did not deter those who for political reasons in 1972 transgressed many of the freedoms guaranteed our people by the Constitution. Few of us would be so naive as to believe that any law, or group of law, no matter how comprehensive or wise, will deter all of those of like inclinations in the future.

But our ongoing efforts to protect and guarantee those freedoms as best we can serve notice to all that if the price of freedom is eternal vigilance, then it is a price we shall willingly pay.

Mr. ABDNOR. Mr. Speaker, in 1896 the captain of the American ship Herbert Fuller was murdered on high seas. After the crime was discovered, Brown, a sailor, was put in irons and the vessel was headed for Halifax, Nova Scotia. Before it reached there Brown charged Bram, the first mate, with the commission of the crime, saying that he saw him do it. Bram was then also put in irons. On the arrival at Halifax, Power, a policeman and detective in the government service at that place, had a conversation with Bram. He testified that he made an examination of Bram, in his own office, in the city hall at Halifax. From the conversation, Bram was indicted at Boston for the commission of the crime.

The conversation, from which a confession of guilt was determined, was the central point of contention in the appeal in Bram against United States argued October 1897. In the decision the court questioned the circumstances of the interrogation.

"Before this examination had taken place the police detective caused Bram to be brought from jail to his private office, and when there alone with the detective he was stripped of his clothing, and wither whilst the detective was in the act of stripping him or after he was denuded, the conversation offered as a confession took place."

Bram had been accused by Brown of committing the crime and the conversation which took place while the defendent was stripped and interrogated by a clothed detective was ruled by the court to be inadmissable evidence of guilt. The court argued that this confession, under these circumstances, could not be considered voluntary and that—

"The impression is irresistibly produced that it must necessarily have been the result of either hope or fear, or both, operating on the mind."

I bring up the issue of this case involving psychological duress because I think it is an important analogy to the situation that occurs every day in the United States. Private citizens of the United States every day go to agencies that extend credit and are confronted by a situation where the loan officer they speak with has a file giving a portrait of that individual's credit standing. These files contain not only records of performance relative to the credit standing of that individual, but also information concerning his personality and history that has mysteriously entered his file without the knowledge of the applicant.

Like Bram, our average consumer has been indicted by an anonymous Mr. Brown. Like Bram, our average consumer goes to be questioned by a credit officer or a job interviewer under phychological duress. Bram's confession was declared illegal because he was stripped of clothing and was interrogated by a clothed investigator. Our citizens are interviewed by a questioner who has information about the applicant and that applicant does not even know what information is in that file. Like Bram, our average citizen is under similar psychological pressure because he is deprived of information which is privy to his request for a job or a loan.

Congress and the courts have an obligation to protect the rights of citizens of the United States. The present practice by organizations and agencies which involves the accumulation of files of information which are used to determine whether an individual will be accepted for a job or for a loan presently puts our citizens under psychological duress.

An example of this was brought strikingly close to the homes of my constituents in South Dakota. The Department of Agriculture requested and received permission to privately audit, examine and process the private tax returns of farmers in South Dakota and across this country. Farmers were to be subjected to, what is in my mind, the unjust and illegal perusal of their private, confidential tax returns. This is exactly my point of contention. Private citizens, in this case honest farmers, were deprived of their rights of privacy and due process by a Government agency which sought to accumulate information and use that information in dealings with these individuals. Their intentions may have been honorable. Their intentions may have been designed to serve the general welfare of the country. But the point remains that the privacy of our citizens was violated. The right of due process was abrogated, placing these individuals under psychological duress.

We are here today to discuss the importance of privacy and confidentiality. There is a need for us to protect the privacy of individual citizens whose rights

are being violated by the accumulation of information and data and the processing of that information which critically affects their opportunities in the social and economic life of this country.

There will continue to be huge data banks of information on individuals in this country and this information will continue to be used to determine acceptability for requests for job employment or credit application or what have you. But the individual has the right to protect himself from misuse of this information. Our citizens have a right to know the contents of the files which are pertinent to their requests.

I hope that Congress will begin to seriously look into adopting measures to protect the privacy and rights of our citizens where these vast systems of data accumulation and processing affects his welfare. I urge Congress to begin investigation into ways of insuring that information accumulated without the knowledge or consent of individuals in this country does not prejudice his rights to due process and privacy. I urge Congress to begin now to protect the rights of confidentiality and privacy of all our citizens.

Mr. MOSHER. Mr. Speaker, I am pleased to be one of those participating in this unique and important special order on the Congressional Committee to Privacy, although I admit to doing so with somewhat mixed emotions.

On the one hand, those of us here today must extend our deepest gratitude and congratulations to those Members of this House who have worked so long and hard to put this forum together. They deserve enormous credit, for they have done their work well. I am confident that this special order will stand for some time as one of the principal records of the Government's responsibility in the area of privacy.

But on the other hand, none of us can take much joy from the fact that here we are, on the floor of the U.S. House of Representatives, trying to make some sense out of why it is that we Americans are apparently watching the erosion of one of our most fundamental rights—the right to privacy. That process of erosion is a profoundly important and compelling development of our age. It strikes at the very heart of our constitutional system.

I intend to outline later in these remarks legislation that I will be introducing to provide a new and significant dimension to the guarantees that come to all Americans as a result of the fourth amendment.

The erosion of privacy is a hydraheaded monster. It takes many forms—from the distribution and selling of mailing lists, to the collection and storage of information by the Government, to wiretapping and other technically sophisticated invasions of our lives.

It seems to me that this latter invasion—the invasion of our freedoms as guaranteed under the fourth amendment—is the most profoundly important area of concern we are considering here.

When Government agents are turned loose at the whim of bureaucrats and politicians to search our homes, seize our papers, and tap our telephones without any prior judicial approval, the most important liberties of a free people are eroded.

Those who founded our country, and presumably those who defended it in World War II, understood the importance of these liberties. Searches by the King's revenue agents in the 1700's and knocks on the door in the night in Nazi Germany were repugnant to our ideas of individual rights. In an important way, that was what World War II was all about. We fought to preserve our right to speak, our right to worship, and our right to vote. No less important is the right to remain secure in our homes.

Under our form of government, unreasonable searches and seizures are not cleansed by being wrapped in claims of national security. Surely, every official can convince himself that his action is important to the well-being of the Nation. In America we cherish individual freedom so much that the test is not whether the official can convince himself—but whether he can convince a judge.

On June 15, 1970, the President of the United States, by his own admission, approved a plan to tap our phones, to open our mail, and to engage in surreptitious entries—all without court approval.

It has been claimed by the White House that this plan was never implemented, and that it remained in force for only 5 days, when it was rescinded.

But there is every reason to believe now that every activity described in the 1970 plans was then undertaken by our Government.

An Intelligence Evaluation Committee was created which conforms precisely to the Intelligence Activities Group (IAG) of the 1970 plan.

An FBI memorandum dated September 16, 1970—only 3 months after the approval of the 1970 plan—for the first time approved the use of campus sources, aged 18 to 21.

Surreptitious entries were undertaken, such as at the office of Dr. Fielding. Other unexplained entries have occurred at the home of CBS newsman Dan Rather, the office of ABC newsman Bill Gill, at the office of Senator Lowell Weicker, and other places where Watergate related material was seemingly the object of the entry.

Telephones have been tapped as in the case of columnist Joseph Kraft.

Mail of American civilians has been opened as demonstrated by documents secured by Senator Weicker.

Apologists for the 1970 plan have attempted to defend it under the cloak of national security a vague doctrine which when unchallenged can too often lead to the gross abuse of individual freedom. The extent to which the national security concept has led to an erosion of our constitutional guarantees was demonstrated on July 25, 1973, when Senator Herman Talmadge of Georgia asked John Ehrlichman whether the national security concept was broad enough to authorize a President to approve murders. Ehrlichman replied, "I do not know where the line is, Senator." The idea that our constitutional rights may be invaded by moral eunuchs who cannot foreclose even murder is nothing short of appalling.

Senator Talmadge also asked Mr. Ehrlichman whether he remembered from his law school days "a famous principle of law that came from England and also is well known in this country, that no matter how humble a man's cottage is, that even the King of England cannot enter without his consent." Ehrlichman replied, "I am afraid that has been considerably eroded over the years, has it not?"

Such invasions of our personal security, and such distortions of the national security concept, offend our most historic freedoms. In 1765 Lord Mansfield established the proposition that the judgment of an independent magistrate is necessary before such rights can be invaded.

In 1772 the Committee of Correspondence of our Thirteen Colonies prepared a List of Infringements and Violations of Rights. Revenue officers of the King had been invading their homes and conducting searches without any judicial approval. The committee wrote:

"Thus our houses and even our bedchambers are exposed to be ransacked, our boxes, chests & trunks broke open ravaged and plundered by wretches, whom no prudent man would venture to employ . . . whenever they are please to say they suspect there are in the house wares &c for which the duties have not been paid."

Before our Constitution was adopted, colonial legislators provided protection to the citizen against unlawful searches and seizures by executive officers. The Pennsylvania Declaration of Rights of 1776 provided in article X:

"That the people have a right to hold themselves, their houses, papers, and possessions free from search and seizures, and therefore warrants without orders or affirmation first made, affording a sufficient foundation for them, and whereby any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his or their property, not particularly described, are contrary to that right, and ought not to be granted."

Similar provisions were found in the Virginia Declaration of Rights of 1776, the Delaware Declaration of Rights of 1776, the Maryland Declaration of Rights of 1776, the Massachusetts Declaration of Rights of 1780, the New Hampshire Bill of Rights of 1783, and the Vermont Declaration of Rights of 1777.

Our Founding Fathers, looking at the abuses in England and Colonial America, desired to protect the individual from officious searches and seizures by bureaucrats and executive officers. They provide in the fourth amendment that—

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Mr. Ehrlichman to the contrary notwithstanding, these historic safeguards have vitality even today. In United States against United States District Court for the Eastern District of Michigan, Mr. Justice Powell held on June 19, 1972, for a unanimous court that—

"These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely with the discretion of the executive

branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility is to enforce the laws, to investigate and to prosecute. *Katz* v. *United States, supra*, at 359–360 (Douglas, J., concurring). But those charged with this investigation and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."

He also stated that—

"The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government. John M. Harlan, Thoughts at a Dedication: Keeping the Judicial Function in Balance, 49 A. B. A. J. 943–944 (1963). The independent check upon executive discretion is not satisfied as the Government argues, by "extremely limited" post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time tested means of effectuating Fourth Amendment rights. *Beck* v. *Ohio*, 279 U.S. 89, 96 (1964)."

He concluded by pointing out the dangers of official surveillance which has not received prior approval of a court:

"Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gatherings, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure."

The issues which Mr. Justice Powell addressed were not hypothetical. The real tragedy of Watergate is not to be found in the breaking and entering, the plans for prostitution, the payoffs, or the perjury. It is instead, a personal tragedy which we all share. It is the erosion of our constitutional liberties which we inherited as a free people.

This threat to liberty did not steal upon us in the middle of the night on June 17. It germinated in the Red scare, after World War I.

It was nurtured as we allowed our government to round up thousands of loyal Americans during World War II—Americans whose only crime was their Japanese ancestry.

And it grew during the 1950's when good men fell silent before the rage of Senator Joe McCarthy.

So we were ready for the maturity of the assault on our Constitutional rights which was uncovered in the wake of Watergate.

The time has come for us to decide. We either believe in the fourth amendment or we do not. If we do, and if the American people are to retain these safeguards, we must act now to give them meaning to our fourth amendment guarantees. We must be sure that never again, can any executive officer, on his own, open our mail, tap our telephones, or break into our houses on the pretext that it involves national security. When national leaders would subvert our liberties in the name of "security," we should remember the words of a letter from the Pennsylvania Assembly to Gov. Robert Morris in 1755:

"Those who would give up essential liberties to purchase a little temporary safety, deserve neither liberty or safety."

Mr. Speaker, I can report to the House that legislation is now being prepared to meet "head on" this aspect of the crisis of privacy. Although I am not now in a position to release the details of the prospective bill, for it is currently only in final draft form and several perfecting adjustments are still necessary, I can promise the Members that it will provide a new, and I believe a welcomed, initiative to shore up the American public's sagging confidence in its institutions of government.

The legislation I am speaking of is being put together by our former colleague, now the senior Senator from Maryland, Charles Mathias. He has indicated to me

that he will be introducing his bill in the near future, and he is especially anxious that any and all Members of the House who may wish to join his effort be given an opportunity to do so.

Briefly, this legislation will call for a mandatory Federal court order before the Government is permitted in any way to intercept communications, conduct electronic surveillance, surreptitious entry, open mail, procure records of telephone, bank, credit, medical or other business or private transaction.

Additionally it provides—and this is of critical importance—that all such court orders, together with official transcripts of the appropriate court proceedings, shall be forwarded to the Committee on the Judiciary of both the House and Senate for proper review.

That provision assures that the Congress of the United States will assume a necessary and proper role in assuring that the protections guaranteed to all Americans by the fourth amendment are not subverted, ignored or in any other way mishandled by either of the other two branches of Government.

Mr. McCLORY. Mr. Speaker, recently I introduced a bill to regulate the dissemination of criminal justice records (H.R. 13164). The right to privacy has gained well-deserved recognition lately, and I am pleased to participate in this special order today on the subject of congressional commitment to privacy.

While recognizing the right to personal privacy in noncriminal areas, this bill does not seal up the records and thus handcuff the police. The arguments for not sealing up arrest records after a certain number of years are persuasive. The premise of the argument is that while rights should be protected continuously, if those rights are not being violated or offended, there is no compelling reason to restrict harmless action not inconsistent with those rights. I know of no empirical evidence to suggest that law enforcement agencies through the country are abusing the use of criminal justice records.

In an effort to protect society as a whole, all criminal justice records should be available to law enforcement agencies to afford them adequate tools in performing their safeguarding function. The right of privacy is not abridged when the police use their own records to investigate suspected offenders of the law.

As all citizens, one convicted of a previous crime has a right to privacy. This right to privacy should guarantee that the record not be used for certain nonsensitive, civil employment situations, but, Mr. Speaker, I believe that one convicted of a crime forfeits his right to privacy at least with respect to the criminal record resulting from the the commission of and subsequent conviction of the crime.

Mr. Speaker, many have discussed the potential for abuse in this area. The possibility for abuse of this information, as long as it is confined within law enforcement agencies, is minimal, especially when the value of this information to the agencies is considered.

I am sure that FBI Director Kelley was in agreement with this notion when he testified before the subcommittee considering this legislation that—

"If only ten murderers or kidnappers repeated their crime outside the statutory time frame, is not this enough to warrant criminal justice agencies access to offender records which might provide leads in subsequent murder or kidnapping investigations?"

I hope, Mr. Speaker, the Judiciary Committee will carefully weigh the several proposals before it and arrive at a balanced recommendation on this important subject.

Mr. McKINNEY. Mr. Speaker, today's special order to express the congressional commitment to privacy could not have been scheduled at a more opportune time. For there is no subject of greater concern to each and every American today than the right to privacy.

This right covers a host of areas. It includes our right under the fourth amendment to be secure in our persons, houses, papers, and effects against unreasonable searches and seizures. It means security in being able to control the collection and distribution of information about oneself. It means confidentiality in bank transactions. It means being able to make telephone calls without fear of wiretaps. It means freedom to say, do, and believe what one wishes without fear of surveillance. It means contributing to causes and organizations without fear of being included on someone's enemies list. In short, privacy is a personal freedom, the citizen's right to live without interference from others.

The American's concern over privacy stems not just from Watergate revelations—although these have enhanced our citizens' fear of "Big Brother" Government—but has been compounded over the years for hardly a day goes by that

some new outrage is not reported. For example, this past Sunday's Parade magazine carried an article relating to incredible consequences which may befall an adult merely because of records kept on him as a child in elementary school.

The American experience, ever since the days of our Founding Fathers, has been imbued with the spirit of personal rights and liberties. This spirit developed from the history, character, and the circumstances of the frontier and has been reinforced by the millions who came to us to escape some form of oppression in their native lands—social, political, religious or economic. They wanted to escape restrictions of one sort or another which prevented them from being or doing or believing what they wished. They enriched American life in many ways but perhaps most of all in their passionate devotion to the concept of freedom as it has developed here. That concept is embodied not only in the Constitution and the Bill of Rights but also in a way of life. To them it meant the inherent right to make what you can of yourself in every way, without being told what to think, do or say, and without fear of Government reprisal.

But what of the present situation? In the short space of less than 200 years we have witnessed the consistent erosion of the basic right of privacy. We are now a great industrial nation of a wholly different type from the America in which the American concept of freedom had its genesis and growth. Jefferson thought democracy and our ideals of liberty would fail when our population became "piled on each other" as in the Europe he knew in his time. Have we reached this stage? Do the economic and technological changes we have achieved necessitate corresponding changes in what men consider freedom? Does our computer technology necessarily mean depersonalization and a loss of freedom for the individual American? Does our urban society mean we are to be constantly subject to barrages of intrusion into our private lives? At this point in our history we must determine whether we are to be a people who controls their Government or a Government that controls its people.

My interest in the issue of privacy is not recent. In fact, one of the first bills I cosponsored when I came to Congress in 1971 was a privacy bill, designed to guarantee an individual's knowledge of and access to records concerning himself which are maintained by Government agencies.

However, Mr. Speaker, I must admit I had not realized to what extent there was citizen concern about privacy until recently when one of my older constituents, distressed over medicare reimbursement, refused to give me his social security number so I could check with the Social Security Administration regarding his case. Very simply, my constituent feared Government retribution. How could I assure him that seeking information regarding medicare is his privilege as an American citizen, that in a democracy he has the right to seek clarifying information and to secure a hearing, if necessary, on his complaint? How can I assure this citizen and the many others who share his fear that his name would not be included in a file as a potential trouble-maker? How do I assure him that his is a Government committed to protection of individual rights and liberties? My constituent has been reading the newspapers and listening to news reports; he knows, as we all know, that simple acts, statements or inquiries can and have been interpreted in a different fashion than intended and have been included in Government dossiers. He knows, as we all know, of the host of actual and potential intrusions into individual's private lives, from political surveillance to computer data banks and the expanding use of social security numbers as a means of identification.

Today there is fear among our citizens because of the abuses of the individual right to privacy. And this Congress must act to conquer that fear. For fear in itself is degrading; it easily becomes an obsession; it produces hate of that which is feared. Already there is citizen distrust; already there is citizen fear; are we to live to see citizen hate of their Government because of fear? While eternal vigilance is the price of liberty, our lot today seems to be eternal anxiety about our liberty.

But mere concern, mere prating about privacy will get us nowhere.

We must enact legislation to control all kinds of automated files on individuals, for the mushrooming unguarded, uncontrolled data banks pose an obvious threat to civil liberties and the potential for injury is magnified by the very real possibility that a person's record will be inaccurate or misleading. I speak not just of Government computer systems but the programs of private industry as well. The privacy problems posed by the $20-billion data-gathering business and the 7,000 or so Government computers which hold information on citizens' private lives is enormous.

Congress can make a start toward fulfilling our responsibilities in this area by enacting legislation curtailing the use and dissemination of criminal arrest and other law enforcement records, particularly the FBI's National Criminal Identification Center's program. While I believe it is important that the FBI compile pertinent data for effective crime control, I question the registering of names and actions of all persons who have any kind of contact with law enforcement officials. When a system includes unproven accusations, arrests not followed by convictions, allows agencies not connected with law enforcement to have access to these confidential records; when people without criminal records are recorded for noncriminal acts, suspicions or for political beliefs, then we have an intolerable violation of privacy and civil liberties.

We must give a conscience to our computers and deal with our citizens as individuals, not as numbers on a card. Retention in data banks of every aspect of our lives, including uncorroborated statements with no opportunity for the individual to review and correct his record, has a very chilling effect on the full expression of first amendment rights.

Congress must take steps to protect the privacy of bank records and credit ratings; make major improvements in the Fair Credit Reporting Act; protect the confidentiality of the individual tax return so these forms will no longer be used as a tool of Government harassment. We must also limit decennial census questions to prevent unnecessary and undue invasion of the Government into the privacy of its citizens.

The growing use of the social security number as a means of identification not relating to the individual's social security account, is an issue of gravity to be investigated. Even the practice of the Government selling mailing lists of names and addresses of individuals to private commercial businesses can be an invasion of privacy. Individuals should have the right and a practical means of preventing the Government from including them on such lists.

Undoubtedly most difficult of all our tasks, we must come to grips with the problems raised by illegal and improper wiretaps, political surveillance, domestic spying plans, illegal search and seizures, infiltration and harassment of dissident groups, use of agents provocateurs, and the whole raft of related abuses which have come to public attention in the past few years. Such actions constitute a brutal attack on our Bill of Rights, on our right of privacy. Government surveillance of political activity stifles the free expression of ideas and discourages participation in the political process, the very basis of our democratic system. Congress cannot avoid the hard decisions of how the Government's police powers ought to be used and what kinds of investigations, by what agencies, are necessary and legitimate. A limit must also be found and placed upon what can be done in the name of "national security."

Concern over protection of the right of privacy has been evoked by representatives of the entire political spectrum, from those labeled conservative to those considered liberal. Indeed, this is an issue that transcends all labels for it is an issue fundamental to our system of Government, intrinsic to our individual liberties and to our future as a democracy. Innumerable articles have been written on the issue of privacy, advocating various approaches and solutions to the problems we face; advisory committees have been established within the various Federal agencies and they have issued reports, most notably the Department of Health, Education, and Welfare's report on "Records, Computers and Rights of Citizens." Innumerable legislative proposals have been introduced in the Congress on the subject of privacy. Certainly with this wealth of materials at hand the Congress can band together and enact meaningful and effective legislation in this field, to insure that the abuses that have occurred are not repeated, to insure that our right of privacy does not become a mere abstraction.

Mr. Speaker, today we express the congressional commitment to the right of privacy. Let us give meaning to our words by meeting our responsibilities, enacting legislation to insure that the constitutional guarantee of privacy is more than just words and thus reinstill in our citizens confidence that their Government does indeed respect the freedoms guaranteed in the Constitution.

Mr. MOAKLEY. Mr. Speaker, I join my colleagues on both sides of the aisle in urging Congress to enact legislation which will guarantee every American protection of our right to privacy. This special order is evidence that there is growing bipartisan support for this legislation to be passed into law.

If this legislation is to be effective, it must apply to all of the information maintained under an individual's name, and all information kept in other files. It must apply to information obtained from an individual, and information obtained from sources other than the individual whose files it is in.

We must not allow the serious problems which have resulted from the introduction of computer technology into the area of recordkeeping eclipse many other equally important issues.

A vast amount of information is still maintained in manual files. Even though the data in these files is available from one source, and computer files are available from many, sometimes hundreds of sources, manual files must be as carefully controlled as computer files. All personal dossiers maintained by Federal agencies must be strictly supervised if every American is to be sure that the Federal Government will not invade his or her privacy.

Even more importantly though, the information gathering process must be carefully controlled. Unnecessary information must not be collected. Inaccurate data must not be retained.

For example, we should direct our attention to the misuse of the postal service and the telephone system as means of gathering personal information. The information gathered from these sources, by tracing who contacts who, is often misleading. It is clearly an invasion of the right to privacy. Legislation must control the use of these services, and other inaccurate means of collecting data.

We must determine when it is propore and necessary for data to be collected, and how it may be collected. We must decide what constitutes improper information gathering, and when it should be illegal.

Equally important to regulating the means of data collection, is the need to monitor the accuracy of the data collected. Every individual must be permitted to see files maintained under his or her name, and information on themselves maintained in files under other names as well. Everyone must be made aware of the existence of his or her files.

People must be able to challenge Federal agencies that certain data should be removed from their files because it is either inaccurate or misleading. In order for this to be feasible, a regulatory board will have to be established.

An individual must be given ample notice before his or her file is released, so that an appeal of the decision to release that file is possible.

This legislation should require that every agency keeping personal records establish strict rules regulating the distribution of information contained in their files. These regulations should then be approved by Congress. Congress must maintain oversight in this area.

For Congress to consider regulations of hundreds of agencies would be a cumbersome task. This task would be greatly simplified if a board were established.

It is important that this board be independent of other Federal agencies. It must be composed of representatives from the broad spectrum of people involved in law enforcement, civil liberties and the legal profession. It must not become an arm of either the FBI, or of the Justice Department.

A complaint often heard against this proposal is that the cost would be too great. I find this response unsatisfactory. This board will be small in light of other Federal agencies and boards, and its function is vital. I do not see how anyone respecting the Constitution can say that freedom is not worth the price of this board.

Whatever guidelines we set up will be insufficient. The same is true for regulations adopted by Federal agencies. There must be a regulatory board to make decisions on individual cases as they arise. It is to the advantage of both Government agencies and people whose files are concerned for this board to exist to expedite the decisionmaking process.

Law enforcement officers often cannot afford time delays. Most people would not bother to appeal decisions for their files to be released or to have information removed if the appeals process were complicated.

I am inserting into the record information relating to the Massachusetts experience with a regulatory board.

Because Massachusetts has been in the forefront of the fight to protect the right to privacy, I am aware of the struggle which exists between the Federal Government and State and local governments in the area of recordkeeping. Massachusetts has refused to participate in the FBI's National Crime Information Center because of this conflict and has also risked losing many benefits offered by the Federal Government because of this.

Massachusetts law provides that records shall be carefully scrutinized before they are released. Massachusetts provides for the expungement of many types of criminal records after a period of time and does not keep a record of unsubstantiated accusations.

The NCIC computer, on the other hand, keeps all of this information. After an individual was no longer in the Massachusetts criminal files, he could very well remain in the SCIC files and his record—forgotten by the State with the authority to prosecute him—will be retained by the Federal Government.

This raises two very serious questions. The first is a constitutional problem. Why should the Federal Government have control over data collected by States fulfilling the constitutionally mandated responsibilities? The answer is that it should not. This question is not limited to matters of criminal histories either. All records kept by States to help implement their laws should be under those States' control.

If a State feels that those records should be expunged, then the Federal Government should automatically expunge that same information.

The second question is a practical one which arises directly out of the problem I have just described. How can a State protect the rights of its citizens by carefully regulating the release of data unless there are correspondingly strong Federal rules? As long as the information in a State's files is available through Federal data banks to hundreds, if not thousands, of Federal, State, and local officials, a State cannot. That is why Massachusetts has been unwilling to participate in the NCIC or in other national data centers.

If every State in the Union passed strict laws to regulate the release of personal data, those laws would be worthless unless there were correspondingly strong laws on a national level. It is imperative that the national laws be as strong as the strongest State laws, and that they be enforceable.

I hope that the day is not too far away when we will rise in support of a bill which will guarantee every American his or her right to privacy. It is important that this legislation be considered soon, but it is also important that this issue be treated comprehensively, and with great care.

As you well know, what we are dealing with is basic to the American concept of freedom. The rights of every individual are sacred to the people of the United States. And we as legislators must also hold those rights to be sacred. What is at stake is the very essence of our democracy.

[The information follows:]

TESTIMONY ON PROPOSED REGULATIONS FOR CRIMINAL JUSTICE INFORMATION SYSTEMS

(By Arnold R. Rosenfeld)

I would like to thank the Chairman for the opportunity to appear here today and comment, on behalf of the Governor of Massachusetts and the state Criminal History Systems Board, on the proposed regulations governing the dissemination of criminal record information and criminal history information.

I will divide my statement into four parts; background, general comments on the content of the regulations, specific problems with the regulations, and suggestions for remedial action.

Let me first provide you with some background on our perspective. We believe Massachusetts has played an important role in encouraging the federal government to come to grips with the important issues to be considered here today.

As a result of our examination and analysis of the information needs and practices of our criminal justice agencies, we recognized that they were at the same time grossly misused by a myriad of other public and private agencies for purposes never originally intended or understood. These misuses included employment and credit checks, social welfare agency checks, and many others.

We, therefore planned out a carefully constructed automated system, obtained legislative authorization for it, and set up strict laws and rules to insure its integrity. We purposely limited discretion, because when you're dealing with an issue as a sensitive as individual privacy, it should not be subject to executive whims.

We recognized from the outset, however, that regardless of how stringent we made the safeguards in Massachusetts, if we participated as planned in NCIC, they were only as good as what would exist in other states or in the federal government. And we recognized that such participation would be to our advantage.

Since we felt strongly about privacy, we wanted to be sure that the federal government and other states understood our position. Governor Sargent, therefore, wrote to the Attorney General and expressed our concern. Our Criminal History Systems Board carried out our statute, which had strong privacy provisions. We were rewarded with a suit brought by the Small Business Administration and the Defense Investigative Service.

We pressed on, however, Governor Sargent joined in a petition to require the Justice Department to promulgate regulations. This petition stressed privacy concerns and the need to regulate NCIC especially. The suit was dropped and we were informed that legislation was being drafted and that rules would soon be promulgated.

We believed that we were being hard. It is now clear that we are not being taken seriously and that the commitment of this administration to improved privacy of data banks is just words.

In the introductory statement of these regulations, we note that the "purpose of these regulations is to afford greater protection of the privacy of individuals who may be included in the records of the FBI, criminal justice agencies receiving funds directly or indirectly through LEAA, etc."

In our opinion, Mr. Chairman, this is the closest these regulations come to requiring th FBI to do anything to protect anyone's privacy as far as its responsibility is concerned with NCIC.

These regulations require the states to develop a plan within an extremely short time and to file a series of reports on action to be taken. The requirements are quite comprehensive, and except for a few specifics, we generally agree with them.

Subpart C requires nothing by the FBI. It is a statement of what they presently do now in operating NCIC. The only new items are section 20.33 and 20.34, which limit access and dissemination and provide the individual the right to look at his own record. There is no interpretation of the issues raised by these two items, which are extremely complex. In our draft regulations, interpretation of these two matters took more than thirty pages.

It is clear to us that the Department of Justice has not understood the concerns of the petition, or it has missed the whole issue, or the President's statements on privacy have no meaning. We wanted regulations to govern this system, not a description of the system. We wanted interpretations and definitions, not a statement about the discretion of the Director of the FBI. We wanted procedures to correct mistakes and remedy inaccuracies, not a statement of regulations that were already in existence.

Let me now be specific.

Section 20.2—The Definitions—we believe raises some problems. Section 20.2 (b) is completely inadequate. It does not define intelligence. This is essential because of the sensitivity of this type of information. Criminal justice agency, as defined in 20.2(d), uses the principal function test. We found this to be confusing without further specification. The sealing provision does not really involve sealing, if it allows the information to be used by criminal justice agencies.

We feel we can comply without great difficulty with Subpart B, with one exception. Section 20.22(a)(1) includes access by agencies authorized by federal executive order. This is contrary to our statute. So is section 20.33(b) which is similar. We do not believe federal executive order should be able to overrule states' statutes. If these agencies have a legitimate right to these records, let them go to the Congress for the authority, as was suggested by the previous Attorney General.

I believe that most other states will have difficulty meeting the requirements of Subpart B, but we will not.

Subpart C really defies specic comment. It does not even purport to regulate NCIC. I will comment only on Section 20.35, which establishes the Advisory Policy Board. It is solely at the discretion of the Director of the FBI, and while it provides for broader representation than before, it still is police oriented. In any event, the Advisory Committee really has no power.

As a result of our review, we believe that the Department should actually prepare regulations governing the NCIC system. These regulations place great burdens on the states and more on the federal government. If this system is to truly operate so as to achieve the purpose stated in the introduction, then both the federal and state governments must establish careful safeguards.

Mr. BAFALIS. Mr. Speaker, anyone who has ever read George Orwell's classic "1984" has expressed dismay at the complete lack of individual privacy portrayed in the book.

This sense of outrage transcends political philosophy.

One's right to privacy is a very basic, almost innate instinct. It is also one which has been the hallmark of all free forms of government. In fact, the individual's right to privacy makes the most definite distinction between freedom and totalitarian or communistic forms of government.

Unfortunately, we seem to be confronted now with a serious erosion of this right to privacy in our society. While we in the United States have not yet reached the state where television cameras constantly monitor every move we make as was the case in 1984, there is little doubt that our personal privacy is being threatened.

In recent years, there has been a tendency on the part of big government and big business to encroach upon the individual's right to privacy of information about his activities, his finances and his lifestyle in general. Computers and data banks all over the country are chock-full of details concerning the background of millions of Americans.

This can only be viewed as a very dangerous trend.

Privacy is defined in Webster's as "the quality or state of being apart from company or observation." In view of the events of recent years, however, perhaps this definition should be amended to read "privacy is the control over the facts and figures of one's own life."

Unfortunately, the problem we are discussing has become so broad that it is virtually impossible for an individual to have this control over the facts of his own life.

Therefore, it is up to the Congress of the United States to take the remedial action necessary to reverse this trend.

And, I am pleased to note, the outlook on this matter is bright. As of mid-March, some 102 bills, sponsored and cosponsored by 207 Members of Congress, had been introduced in the House. In the Senate, various privacy bills have the backing of 62 of the 100 Senators.

I, personnally, have sponsored legislation to protect the confidentiality of individual income tax returns. While it is necessary for the Internal Revenue Service to compile the data on individual returns to insure that all Americans pay their fair share of the cost of Government, there is no reason for that information to be available to anyone else .

It is far past time for the development of a Code of Fair Personal Information Practices to establish safeguards to protect individuals from those agencies which collect information. There have been too many cases of gross inaccuracies perpetuated to the detriment of an individual's credit rating and, more importantly, his reputation.

We should take every possible step to limit the use of the Social Security number as a universal identification number. Bills to accomplish all these goals have been introduced in the Congress, as have a number of others. So the effort is being made.

But more is needed. We, as Members of Congress, must push relentlessly to obtain the legislative action necessary to see that these vital bills are approved by Congress and become public law. Only in this way can we provide the individual with the safeguards necessary to protect his continued privacy.

I am hopeful we will be able to enlist all the Members of this body in a broad, bipartisan effort to see that this is accomplished.

Anything else could well mean "1984."

Mr. COUGHLIN. Mr. Speaker, among the ideals that America was founded upon, perhaps none is more important than the right to individual privacy. Interwoven with the Constitution and the Bill of Rights is the guarantee that every citizen is entitled to the broadest measure of personal privacy. Our judicial system has recognized this right and has moved, at all levels, to preserve and protect it.

However, the continued advance of technology poses the threat of unprecedented invasions of privacy. Sophisticated new techniques have been developed which could not have been foreseen at the time the Bill of Rights was adopted, techniques of information gathering which have become commonplace and are available to overzealous bureaucrats, misguided public officials, and aggressive businessmen.

The individual citizen, who is often unaware that he is being victimized, is virtually helpless to combat this unseen enemy. It is the responsibility of Congress to delineate the rights of the individual confronted with this threat, to legislate protections for him and to restrict and regulate the use of methods of information gathering and surveillance which, by their nature, infringe on the right to privacy and are therefore inimical to our fundamental ideals. Americans should not come to expect that their right to privacy will be infringed. Congress must take the necessary action to insure that this does not occur.

I believe there is an ominous correlation between the growth of huge bureaucracies, including the Federal Government, and a growing sense that it is necessary and proper to obtain information about people and their activities without their knowledge or approval. Personal familiarity with individuals is beyond the capacity of most organizations. Consequently, they resort to questionnaires, computers, data banks, identification numbers, credit checks, or other impersonal means to make judgments concerning individuals which they consider relevant to their business. In this way, invasion of privacy becomes legitimized and accepted as common practice.

This trend is a dangerous one. If allowed to continue unregulated, it will lead to a society in which an individual's right to privacy is all but forgotten. That right is already under attack and we must act now to ward off further encroachments.

As a Congressman who has been apprehensive about this trend, I have sponsored bills to deal with specific situations in which the potential for abuse has been outstanding. I have sponsored legislation to require all Federal agencies maintaining records on an individual citizen to apprise him of the existence of the records, to permit him to inspect them and to furnish supplemental or explanatory information to the file. In addition, I am sponsoring bills which would limit the sale or distribution of mailing lists by Federal agencies and restrict agency access to Federal income tax returns. Responsible safeguards such as these will provide a first step toward insuring that the right to personal privacy will not be violated by the massive Federal bureaucracy where the temptation to impersonalize individual citizens, to gather often unnecessary or irrelevant files, and to share this information freely among agencies, magnifies the potential for abuse.

However, the problem of privacy, like the principle, is not confined to the policies and actions of the Federal Government. It pervades the realm of business relations as well as State and local public policy. Therefore, a piecemeal approach to privacy protection legislation, concentrating primarily on Federal policies, is destined to fall far short of the broad reforms that are needed.

Banks and other credit institutions, law enforcement agencies, and employment bureaus are but a few of the organizations in which confidential information is elicited and in which that information may be subsequently misused. While the Fair Credit Reporting Act of 1970 was a signficant step in eliminating some of the more glaring abuses that have occurred, it is too narrow in scope to implement a national commitment to the right of privacy.

By the same token, the Federal establishment must take the lead to ensure that the privacy of all citizens is respected if meaningful legislation is to be enacted covering the private sector. Regrettably, the actions of the Federal Government have not been exemplary. The past year has been filled with reports of secret dossiers, inspection of tax returns, break-ins, and rummaging of personal and confidential files, as well as surreptitious electronic surveillance on the part of Federal officials. These are surely the most despicable violations of the right to privacy. These are deliberate and knowing efforts to abridge fundamental rights and for this reason are demeaning to those who are a party to them.

Perhaps the most flagrant and abused invasion of privacy has been the unauthorized use of wiretapping. Under the guise of national security more than a dozen officials and newsmen have been admitted by the Justice Department and indications are that the actual number may be even higher. No comprehensive approach to guaranteeing the right to privacy can fail to deal with the sensitive issue of wiretapping. Existing safeguards enacted by Congress as part of the Omnibus Crime Control and Safe Streets Act of 1968 limiting wiretaps to investigations of certain specific crimes and requiring prior court authorization have not been sufficient to curb excesses in this area and further legislation is needed. The violation of civil liberties inherent in telephone taps, invading the privacy of not one but countless unsuspecting individuals, is so severe and so repugnant to our basic rights and freedoms as to be justified in only the most extreme national security emergencies and then only with prior court approval. The task of striking the proper balance between the individual's right to privacy and the exigencies of national security is a difficult one. The Congress can and must play an active role in this determination.

Mr. THONE. Mr. Speaker, on February 7, 1973, I warned that the Executive order giving the U.S. Department of Agriculture power to examine all farmers' income tax returns could destroy America's faith in its tax system.

In a telegram to the President and to Secretary of Agriculture asking that the order be rescinded, I pointed out that this was the first instance of any Federal agency being given power to examine the returns of all people engaged in one occupation. I stressed that other agencies would follow suit if the precedent were allowed to stand. The Federal Communication Commission would be asking for the returns of all corporations and leading executives engaged in broadcasting. The Interstate Commerce Commission would be seeking returns of corporations and individuals engaged in transportation. The Labor Department would be asking for returns of labor union executives.

Two committees of the House of Representatives—Agriculture and Government Operations—held hearings on this matter. I am fortunate to be a member of both committees. As a result of the work of these two committees and of the pressure of Members of Congress on the administration, the Executive order authorizing examination of farmers' returns has been revoked.

I am not satisfied, however. If an Executive order could be issued once, it could be issued again. We must have legislation to protect the privacy of all income tax returns and to prevent their being pawed over by officials of various Federal agencies. I am a cosponsor of proposed legislation that would greatly restrict and control the inspection of income tax returns.

When a person makes out his income tax returns, he may reveal many personal and private matters. Our tax system has been the most successful of any in the world. Our citizens voluntarily tax themselves by completing income tax forms. If the information they impart to the Internal Revenue Service is not held in the strictest confidence, our tax system could be ruined. Most importantly, we must uphold and guarantee the right of citizens to be free from unnecessary and unwarranted snooping into their affairs by Government officials.

Mr. KEMP. I thank the gentleman for taking this time. Mr. Speaker, on some issues before this House, there must be no retreat from our resolve. The insuring of adequate safeguards to protect the individual's right to privacy is such an issue.

When liberty is threatened, no measure is adequate unless it guarantees the protection of that liberty. I am proud, therefore, to cosponsor this special order on the right to privacy.

The right to privacy is the right to be let alone—the right to be left alone. It is a right which forms the basis for such protections as those shielding the individual against unwarranted searches and seizures, electronic surveillance, snooping investigations and "fishing expeditions," and the inspection of personal papers, records, and effects. Much of our Bill of Rights—our first 10 amendments to the U.S. Constitution—is predicated upon this right to privacy.

Support for the individual's right to privacy is a feeling which runs deeply in the spirit of our Anglo-American heritage. As Mr. Justice Brandeis observed in his 1928 opinion in Olmstead against United States, the makers of our Federal Constitution recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure, and satisfaction of life is to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensitivities. They conferred, over and against the Government itself, a right to be let alone—a right to privacy—the most comprehensive of rights and the right most valued by civilized men. It is this right which gives the individual the force of law to say to an agent of the Government, "No, you cannot come into my house or into my life, by any means, without my consent or the full requirements of law and due process."

PRIVACY MEASURES ARE MAKING HEADWAY

Important measures before this House, insuring further the right to privacy, are making headway. As the gentleman from California (Mr. Goldwater) has indicated in his remarks today, as of March 13 there were 207 different sponsors and cosponsors of 102 bills and resolutions in the House in this subject field, with 62 Senators making or cosponsoring similar proposals in the Senate. I think this reflects strongly the concern of Members—and the citizens they represent in these Halls—on this matter.

I have said much on the subject of privacy before today, and my colleagues are making many more valuable contributions to the dialogue on this issue today. I do not wish, therefore, to take the time of this House in simply repeating that which has already been said.

I wish, however, to concentrate my remarks today on a few crucially important items. I speak of these particular, substantive actions:

First, the successful Goldwater-Koch-Kemp amendment to the proposed Federal Energy Administration Act, H.R. 11793;

Second, the announced recission of Executive Orders 11697 and 11709, highly controversial orders which had given the U.S. Department of Agriculture authority to inspect the Federal tax return of farmers;

Third, the consideration of measures to either prohibit or limit the procedural operability of so-called mail covers;

Fourth, the successful amendment which I offered on the protection of pupil rights to the proposed Elementary and Secondary Education Act Amendments, H.R. 69, an issue closely related to the protection of privacy;

Fifth, my intention to offer, at the earliest possible opportunity, remedial legislation addressed to the subject of protecting the privacy of records maintained by school systems on pupils; and,

Sixth, a recent commitment to me by the Commissioner of Internal Revenue to review de novo all IRS procedures and Regulations which might be construed as potentially infringing upon the right to privacy and to insure, in any revisions of those Regulations, that adequate safeguards for protection of that right are required.

Let me comment on each of these matters.

SUCCESSFUL GOLDWATER-KOCH-KEMP AMENDMENT TO THE PROPOSED FEDERAL ENERGY ADMINISTRATION ACT

The right to privacy must be carefully protected, especially so when it could be endangered by the collection, storage, and use of information by Federal agencies. The exchange of information between such agencies, as well as its use as a basis for litigation, requires that such information be gathered under the strictest procedures, stored with full confidence, and used properly.

On March 7, the gentleman from California (Mr. Goldwater) and I cosponsored an amendment to H.R. 11793, the proposed Federal Energy Administration, the intended successor to the Federal Energy Office. That amendment requires that to protect and assure privacy of individuals and personal information, the Federal Energy Administrator is directed to establish guidelines and procedures for handling data pertaining to individuals. He shall provide in such guidelines and procedures a reasonable and expeditious method for each individual data subject to:

Be informed if he is the subject of such data;

Gain access to such data;

Contest the accuracy, completeness, timeliness, pertinence, and necessity of retention or inclusion of such data.

The Administrator shall also take necessary precautions to assure that no indiscriminate transfers of data pertaining to individuals is made to any other person, organization or government agency.

We were supported in the offering of this amendment by the gentleman from New York (Mr. Koch). The breadth of support for measures to further insure the right to privacy can be seen easily from the sponsorship of this amendment: Mr. Goldwater, a conservative; Mr. Koch, a liberal, and myslf, a moderate. This broad, bipartisan support bodes well for the enactment of future legislation.

The amendment was accepted, on a division vote, by a plurality of 86 percent "ayes." That, too, bodes well.

I hope that the Senate will accept the language of this amendment. I urge them to do so. If this bill becomes law, it should certainly carry within its provisions the safeguard amendment we offered.

INQUIRY INTO EXECUTIVE ORDER 11697 AND 11709

There was a time when citizens could assume that, except for examinations by IRS itself, their Federal income tax returns were reasonably safe from the prying eyes of other Federal agencies— whether the intentions behind such searches were malevolent or well-meaning. One knew when he sent in that most personal documents each April 15—your Form 1040 and related papers—that it was a confidential matter just between him and the IRS, unless of course he did something illegal or improper.

Unfortunately, that confidential treatment of Federal tax has been recently endangered. In early 1973, upon the advice of his counsellors and presumably with good intentions, the President signed Executive Order 11697—subsequently amended by Executive Order 11709. These Executive orders allowed the U.S.

Department of Agriculture to inspect—at its option—the tax returns of any—or all—of our Nation's millions of farmers. I will take the Department's recent word that there was no evil intent behind the order, but that disclosure misses the real point of concern. The motive is not important; the effect is.

After all, anyone can develop a rationale for the inspection of tax returns. The Department of Agriculture, in this instance, stated it wanted the information only to compile statistics about farmers that might be useful in formulating farm policies. But such similar "good motives" could raise the possibility of the Department of Commerce wanting returns on businessmen, or of the Federal Housing Administration on homeowners, or the Department of Labor on union members. The list could be endless.

Two Members of this body spotted the dangers of these Executive orders and brought them to the attention of the Members. I think the House owes a debt of thanks to the gentleman from Missouri (Mr. Litton) and the gentleman from Arkansas (Mr. Alexander) for exposing these orders.

The administration has now announced its intention to rescind these two Executive orders. I commend the administration for such action, but it should be viewed only as a first move of many steps which need to be taken to insure adequately the protection of privacy, especially with respect to the confidentiality of tax returns. I believe remedial legislation may still be required.

THE CONSIDERATION OF LEGISLATION TO PROHIBIT OR RESTRICT THE USE OF MAIL COVERS

On March 26, I addressed this House on the need for legislation on the subject of mail covers. This was a matter which was brought to my attention as a result of correspondence and discussions with attorneys and professors involved in the privacy issue.

What is a mail cover?

In a mail cover, information appearing on the outside of envelopes intended for a specified addressee is recorded, without his knowledge, by postal employees before the letters are delivered. The addressee has no idea that this information is being recorded about his incoming mail; that mail simply is left in his box or office each day, as usual. This information, which includes the postmark and return address of the addressor, is then given by the postal service to the Government agency which requested the cover be imposed.

What makes the use of mail covers an unconscionable practice is not only that they invade a person's right to privacy but also—because they are perceived even by the agencies using them as being of questionable color of law—that their use is seldom ever disclosed in a trial for fear that evidence ascertained through them will be ruled inadmissible. But, the evidence is used, nonetheless, without making disclosure of from where the authorities first got an indication of the existence or nature—the mail covers.

Since disclosure of the use of mail covers is suppressed, no one has an accurate fix on the extent of their use. Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, conducted in 1965, showed an acknowledged existence of 730 separate covers on a date certain in 1964. That is believed to be substantially greater than the number of wiretaps in effect at that point in time. A 1968 study of the Columbia University School of Law, showed a decline in the number of mail covers in effect, but showed a widespread existence of their possible abuse.

In order to ascertain more accurately the extent of mail cover uses today, I have written to the Postmaster General, E. T. Klassen, asking for current information on the number of mail covers in effect and on the source of the request for the use of those mail covers, per agency.

I have not yet introduced remedial legislation. I did propose in my remarks of March 26 the consideration of a draft text, one which would prohibit outright the use of mail covers. I have not actually introduced remedial legislation to date, however, for I believe a determination must first be made as to which course of action would be the most effective to pursue: Either an outright prohibition, such as that suggested on March 26, or a proscriptive amendment to title 18, United States Code, which would permit the use of mail covers in a specifically authorized set of criminal investigations but only then if prior court approval were obtained. The former would be similar to the current court requirements with respect to the authorization of wiretaps in criminal investiga-

tions, as those basic requirements are now set forth at 18 U.S.C. 2516 (1) and (2) coupled, however, with an additional requirement for prior court approval.

I have solicited the views of the Postal Service on the manner in which it would prefer to move forward with remedial legislation, for I believe strongly the Postal Service could use this legislation to protect itself as much as I want that legislation to protect the individual citizens.

I hope to report to the House the progress on this issue of mail covers at the earliest possible opportunity. I think it merits the attention of all of us.

THE PROTECTION OF PUPIL AND PARENTAL RIGHTS

Nothing could be more intrinsically intertwined with the right to privacy than the protection of the sanctity of mind and body, a sanctity which can be subtly eroded by various behavior modification measures.

On March 27, I offered two amendments to H.R. 69, the proposed Elementary and Secondary Education Act Amendments of 1974. These amendments, which were accepted on voice vote, would insure protections against invasions of the privacy of pupils in our schools and against infringements on parental rights.

These amendments, if enacted into law, require that no child shall participate or be used in any research or experimentation program or project, or in any pilot project, if the parents of such child object to such participation in writing, and that the moral or legal rights or responsibilities of parents or guardians with respect to the moral, emotional, or physical development of their children shall not be usurped in the administration of these programs.

Nothing is more essential to the right to privacy, the right to be let alone, than the right to individuality, a right intrinsic in the moral, emotional, and physical development of each person. Programs and projects which seek to modify behavior, or moral values, or physical abilities—for the purpose of achieving modification as deemed appropriate by the modifier, not necessarily the student or the parent—can invade or infringe upon that right. Too often these programs and projects can lead to either conformity or uniformity of behavior, something which inherently denies the right to be different. And, too often these programs and projects use pupils almost as if they were guinea pigs, to test out the viability of new methods, often forgetting the impact such testing—and the failure of methods—could have on the pupils.

I urge the Senate to accept these amendments and the committee of conference to preserve them in the final version of the bill.

PROTECTION OF STUDENT RECORDS AGAINST DISCLOSURE

Another area of serious concern has begun to surface during the past several months.

I speak of the potential misuse by disclosure of extensive information about pupils, maintained in the various public and private school systems.

What began more than a century and a half ago to keep registers on enrollment and attendances has grown to grotesque proportions.

Educators have constructed elaborate information gathering and storage systems, all in the name of efficiency, adding a piece here and there, tinkering with new components, assuming all the while they were creating a manageable servant for school personnel. But, what they failed to foresee was the swift development of modern technology and the widening employment of that technology by a social system increasingly bent on snooping.

The growth of student records into an all-inclusive dossier came in response to the increasing centralization and bureaucratization of schools. Another contributing factor was the emergence of education's ambitious goal of dealing with "the child." Out of that context grew such specific actions as the National Education Associations 1925 recommendation that health, guidance and psychological records be maintained for—on—each pupil, and the American Council on Education's 1941 development of record forms that gave more attention to behavior descriptions and evaluations and less to hard data on subjects and grades. By 1964, the U.S. Office of Education was listing eight major classifications of information to be collected and placed in the student record.

How much has the system grown? Let me cite my State of New York. Let me cite New York City's public school system as my specific example.

According to a highly informative article by Diane Divoky, entitled "Cumulative Records: Assault on Privacy," which appeared in the September 1973 issue of the magazine, Learning:

[The article follows:]

The ultimate mushrooming of records may have been reached in the massive New York City school system—largest in the nation. There, the records required or recommended for each child involve, if nothing else, a staggering amount of book work. A typical, rainbow-hued student dossier in New York carries:

A buff-colored, cumulative, four-page record card that notes personal and social behavior, along with scholastic achievement, and is kept on file for 50 years;

A blue or green test-data card on which all standardized test results and grade equivalents are kept, also for 50 years;

A white, four-page, chronological reading record;

A pupil's office card;

An emergency home-contract card;

A salmon-colored health record—one side for teachers, the other for the school nurse and doctor;

A dental-check card;

An audiometer screening-test report;

An articulation card, including teachers' recommendations for tracking in junior high school;

A teachers' anecdotal file on student behavior;

An office guidance record, comprised of counselors' evaluations of aptitude, behavior and personality characteristics;

A Bureau of Child Guidance file that is regarded, though not always treated, as confidential, and includes reports to and from psychologists, psychiatrists, social workers, various public and private agencies, the courts and the police;

And all disciplinary referral cards.

The perspective of a Federal legislator here is severalfold.

First, the maintenance of student records is almost totally a matter of State and local jurisdiction.

Second, while there must be protection of the information contained in these records, it must also be available for a sufficient internal use within the school system itself to permit adequate attention to matters involving the actual education of the student.

Perhaps there is an answer. At many colleges and universities, the transcripts of students and graduates are not released unless the student or graduate specifically gives his consent to the release of that transcript to a specified party. That might be a good guide to follow here—that there could be a release of information contained in these records, except for clearly defined internal purposes within an education system or systems, only when the parent or guardian of the student gave written, prior consent, or, once the student has reached the age of majority, he give it himself.

I have this problem under intense scrutiny at this time.

I hope to be able to report to the House and to introduce any appropriate remedial measures at the earliest opportunity.

This is certainly a matter which should not go without redress.

REVIEW OF IRS REGULATIONS

Immediately following the Christmas recess, I had brought to my attention the existence of a number of regulations within the Internal Revenue Service. The possible content of these regulations, but to mention their potential application by agents, concerned me greatly.

On January 7, I wrote to Donald Alexander, the Commissioner of Internal Revenue, making inquiry about the existence and content of the following regulations, which I recite by name and number:

"Methods to Achieve Intelligence Mission, 9141.2:

"Reporting Informant's Communications, 9271.3;

"Confidential Expenditures for Information, 9372;

"Electronic or Mechanical Eavesdropping, 9383.5;

"Surveillance, 9383.7;

"Entrapment, 9385;

"Arrests without Warrants, 9444;

"Search without Warrants, 9452;

"Seizures Incident to Searches without Warrants, 9452.4;

"Electronic Eavesdropping Devices, 241.44; and,
"Use of Raid Kits, 284.51."

A lesson of history is that the most disliked man in any society at any time in history is "the tax collector." I understand that. But, after reading just the titles of these regulations, I began to wonder if maybe there was not more of a reason for that feeling—in our day and age—that we just have to "pay up" each April 15.

I received a response from the Commissioner on February 4, and I want to share excerpts from it with my colleagues today, for they show—according to the Commissioner—that they are efforts to safeguard individual rights and not infringe upon them. Perhaps, but the courts will ultimately have to make that decision. Nonetheless, the Commission stated, in part:

"The various documents cited are not secret; almost all of them are available for public inspection in our Freedom of Information Reading Room in the National Office and have been provided to requesters under the Freedom of Information Act.

"Furthermore, these documents do not contain illegal instructions or promote invasions of privacy, but reflect the Internal Revenue Service's concern that the right of citizens be respected. The instructions are intended to assure fair and proper treatment of investigative subjects. . . . In short our instructions are proscriptive in nature rather than prescriptive. We are now reviewing these documents again to assure that our instructions fully reflect our current practice and goals."

I do not want to be too harsh on the Service, but I think certain things should be pointed out, from practice and from the letter itself.

No regulation is any more self-restricting that the agent using it on a daily basis. With the thousands of agents within the Service—the preponderant majority of which are highly competent, I am sure—can one really be sure that all individuals are safeguarded fully every time one of these regulations is used? Inherent to the size of the Service and nature of the confrontation, probably not.

The fact that "almost all of them" are available does not mean that "all" of them are available. And it is interesting that one must use the processes of the laborious and time-consuming requirements of the Freedom of Information Act to get them—those which are available to the public.

The question of whether they contain "illegal" instructions begs the question, for the fact that they are regulations promulgated pursuant to law makes them "legal." What it does not do is make them necessarily the right law, reflecting the right policies, which should be passed and instituted to protect fully the right to privacy.

The statement that they do not "promote" invasions of privacy is still no safeguard that such invasions are not committed.

Again, I am not here to infer that the Service has made a practice of violating the rights to privacy. I do, however, believe that in a quasiadversarial position between the Government—IRS—on one hand and the taxpayer on the other, that the taxpayer might sometimes not receive full benefit of the allegedly protective regulations.

One particular thing is important—over and above all else: I intend—and I invite other Members to join with me—to hold the Commissioner fully to his commitment that the regulations are, first, under review, and, second, that they will insure adequately the right to privacy.

I use this opportunity, further, to request the Committee on Ways and Means, particularly as it considers such measures as Executive Orders 1697 and 11709, to review the current regulations cited, as well as any revisions made in them. I think such an inquiry would be fully consonant with the responsibility assigned this Body by the Constitution to protect individual rights.

MUCH TO BE DONE

Mr. Speaker, I want to take an additional moment to express my gratitude for the outstanding work which some Members are doing on this issue. I speak primarily of Mr. Goldwater, Mr. Koch, Mr. Horton, Mr. Moorhead, and Mr. Edwards of California. I am pleased to have joined them in many mutual efforts in this regard.

These measures are but small steps—all be they important ones—toward safeguarding the right to privacy. Much more needs to be done.

I am committed to this task, and I invite my colleagues to join with me in this struggle.

Mr. LUJAN. Mr. Speaker, as a participant in today's special order expressing a commitment to privacy, I would like to add my voice to those of my colleagues in support of this fundamental freedom.

I have introduced five separate pieces of legislation on this; the Right to Financial Privacy Act, an amendment to the Freedom of Information Act, a bill to establish a Select Committee on the Right to Privacy, another to prohibit the use of an individual's social security number as a universal identifier, and finally one to provide for fair personal information practices.

The right to privacy of our citizens has been invaded and legislation such as I have sponsored can reverse this trend. We in this country pride ourselves on independence and our individuality; we resent the idea of others having easy access to our records. Furthermore, I believe that the practice of government and private industry establishing and maintaining data banks on citizens is being overused. This has become so outlandish that information about individuals is placed in these data banks from such diverse sources as church records, marriage licenses, pet registrations, hospital and doctor's files, and even hotel registrations.

I am concerned about the irreparable harm and damage many individuals suffer because of the quantity and quality of information collected and used. Much of it is gossip, biased opinion, unverified fact, misunderstanding, and misinterpretation.

I have learned of a case where a man in his mid-thirties was passed over for a major promotion in a large firm because a data bank revealed he had larceny tendencies. This information it was learned too late, came from a prank when he was in grade school. It just so happened that the boy was involved with several others in taking some gym clothes and hiding them in the rafters. There was no indication of other criminal activity in his records.

Collecting and distributing this type of information is not in accord with the principles on which our country was founded, and our work here today can correct this injustice. Let us get started.

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, two of the major issues in Government today are the lack of credibility and invasion of privacy. Our citizens are beginning to question whether our Government tells the truth and, perhaps even more ominous, are beginning for the first time to fear their own Government. These developments constitute an evil trend which the people of any free society can only find intolerable.

On that point, let me say this. The Congress of the United States has a duty like the Supreme Court to interpret the Constitution and make it a living reality. We have a responsibility to do this through the enactment of laws implementing the letter and spirit of that great document. And we are going to do it.

The House Foreign Operations and Government Information Subcommittee is currently considering legislation to make certain that Americans have access to Government files, records, and dossiers kept on them. In all but law enforcement cases leading to criminal prosecutions, and properly classified files, Citizens would have inspection and correction rights.

This landmark legislation, in my view, will be a giant step in protecting the right to privacy—and making certain that Government is the servant of the people and not their master. I hope every Member of this House will support this legislation.

Mr. Speaker, I am proud to be the chairman of the Foreign Operations and Government Information Subcommittee. Its Members on both sides of the aisle are all able advocates of the rights to freedom of information and personal privacy.

Through the years, the subcommittee has conducted pioneer investigations into the Government's use of polygraphs, telephone monitoring devices, and advanced information technology and their implications on the right to privacy.

Last year we conducted an investigation into two executive orders which would have permitted the Department of Agriculture to extract certain personal financial information from the Federal income tax returns of 3 million American farmers. This investigation culminated in revocation of the two privacy-invading orders by the President.

I might say, Mr. Speaker, that the House Committee on Government Operations has shown a deep interest and concern in the protection of personal privacy for almost two decades. In 1964, it formed the Special House Subcommittee on Invasion of Privacy which investigated the psychological testing of Federal employees and schoolchildren, mail covers, electronic surveillance devices, trash snooping, credit bureaus, data banks, and other privacy questions.

Our studies over the years show there is a clear potentiality with the sophisticated and advanced technology of today of almost unlimited invasions of privacy if Government is not carefully watched and checked.

Overall, these inquiries add up to what only can be characterized as a most disturbing picture. Meanwhile, the Watergate investigations have brought out new brush strokes of blackness on the same canvas.

We have heard the details of Tom Charles Huston's White House plan to intensify Government surveillance in the name of improving domestic security. As you may recall, the plan was briefly approved by President Nixon despite its unconstitutionality and objections from the late FBI Director, J. Edgar Hoover. It was later rescinded.

Watergate also brought out the existence of lists of "political enemies" who were to be targeted for income tax audits and other possible adverse Government actions. All of America finally found out to what evil extent the privacy invaders of Government had gone. And it was frightening. The first and fourth amendments contained in the Bill of Rights to the Constitution were under vigorous attack.

But fortunately, the barricades were manned by an aroused Congress, a great and fearless free press and many concerned Americans who put their country above partisan political considerations. In the event any of my colleagues believe I am alleging the privacy invaders inhabit only one administration, they would be most mistaken.

Privacy invasions of our citizens have permeated every recent administration in recent decades. The disease must be eradicated. Each Member of Congress—each citizen—regardless of party—must join together in the battle line to keep it strong—despite who the President is—Republican or Democrat.

My colleagues, we have heard much about preserving the Presidency. I submit the real question is: Are we going to preserve the Constitution?

Mr. DRINAN. Mr. Speaker, when President Nixon announced his support for the right of privacy in the state of the Union message, it was greeted with guarded praise. After all, a great number of the assaults on citizen privacy had been penetrated by officials in the Nixon administration, by his reelection committee, and, in some cases, by Mr. Nixon himself. After reviewing these events in a statement to this body on February 6, 1974, I noted:

"Thus it was with a touch of irony that we heard, in this Chamber a few days ago, a Presidential pledge to take steps to protect the right of privacy. While we can rent about the demogoguery of it all, perhaps the wisest course is to note that we may have gained another ally in the battle against governmental excesses."

Recognizing that Nixon statements in the area of civil liberties are frequently not implemented in practice, I added: "But time will demonstrate whether Mr. Nixon is merely a sunshine patriot and summer soldier."

Since that state of the Union promise, Mr. Nixon has had myriad opportunities to advance the protection of privacy. On those occasions, he has given the American people half measures supported by half truths. Each time Mr. Nixon could have struck resounding blow for securing citizen solitude, he merely administered a wrist slap. It is now clear that, when it comes to the battle against access to matters considered confidential by our constituents, Mr. Nixon and his appointees are indeed a troop of summer soldiers.

For the past several weeks, the Subcommittee on Civil Rights and Constitutional Rights of the House Judiciary Committee, of which I am a member, has been holding hearings on proposals which would regulate the storage and dissemination of data collected by criminal justice agencies. One of those measures under consideration, H.R. 12574, is the Administration bill introduced on February 5, 1974. I should note that the interest of the subcommittee, under the able leadership of Don Edwards, in this subject antedates the administration bill by many, many months. We conducted hearings last session, for example, without any support from the Nixon administration.

Thus I was surprised and pleased when H.R. 12574 was introduced on February 5 and when Attorney General Saxbe appeared on February 26 to endorse at least some measure to guarantee the right of privacy by regulating the storage and distribution of criminal records. The problem, needless to say, is enormous. The FBI alone maintains almost 160 million sets of fingerprints, and arrest records of a substantial portion of those individuals. Arrest data, with or without dispositions, are in turn circulated to any Federal agency which requests them, to State and local agencies for law enforcement, employment, and licensing purposes, and to certain banking institutions. In addition a number of other Federal agencies,

such as the Department of Defense, maintains files on individuals which are distributed to other Federal agencies—and perhaps other non-Federal institutions.

The testimony by Mr. Saxbe unfortunately was misleading and uniformed. He was unaware, for example, of the restrictions which a decision of the U.S. District Court for the District of Columbia placed on the dissemination of arrest records. In *Menard* v. *Mitchell*, 328 F. Supp. 718 (D.D.C. 1971), appeal pending, the court enjoined the Department of Justice from distributing the plaintiff's arrest record to other Federal agencies not engaged in law enforcement—except for employment purposes—and to State and local agencies not engaged in criminal justice activity. That decision is presently on appeal to the U.S. Court of Appeals for the District of Columbia.

Provisions on the administration bill, H.R. 12574, would drastically alter the decision in Menard. The bill allows for the distribution of arrest records—if a final disposition has not been reported—to Federal and State agencies—and even private institutions—for purposes unrelated to law enforcement if authorized by State or Federal statute, or by executive order. In addition Mr. Saxbe failed to inform us that some of these non-Menard uses may unfortunately still be authorized by provisions of appropriation bills. For example, the Supplemental Appropriations Act of 1972 permitted the FBI to disseminate arrest data which Menard had prohibited.

Clarence Kelly, Director of the FBI, provided even less support for the protection of information collected by criminal justice agencies. With respect to fingerprint cards with arrest data, the present policy of the FBI is to destroy them when the individual reaches the age of 80, or 7 years after death, whichever comes first. Even the administration's weak bill would modify that practice to some degree. Yet Mr. Kelley was not in favor of it. He was totally against any provision which would limit access by law enforcement agencies to arrest records, even if the arrest resulted in no conviction, or no further action was taken by the prosecuting authorities.

Finally the subcommittee also received testimony from David Cooke, Deputy Assistant Secretary of Defense, on the same subject. Although the Department of Defense—DOD—is not, according to Mr. Cooke, in the law enforcement business, it nonetheless would like unlimited access to arrest data compiled by the FBI and other police agencies. DOD argues that such information is vitally important in determining employability, whether an employee should be retained, and status for security clearance purposes. At the same time, DOD concedes that it has never denied employment, severed an employee, or refused clearance solely because of an arrest, or even a conviction record.

Why then does DOD want the material? "So that we have a picture of the whole man," responds Mr. Cooke. That, of course, was presumably one of the reasons why the plumbers entered the office of Dr. Lewis Fielding seeking the psychiatric records of Daniel Ellsberg. And presumably why the plumbers—or the White House or whoever—allegedly kept a tap on Morton Halperin's telephone many months after he had left Government service—and while he was advising Democratic Presidential candidates.

One of thhe most ominous parts of Mr. Cook's testimony was his proposal to amend the pending bills to prohibit State and local governments from imposing more stringent safeguards on arrest data. In other words, Federal agencies would have unlimited access to local arrest records no matter what restrictions are imposed by State law. And that suggestion is not made benignly. Mr. Cooke testified that DOD could not complete employment or security checks of citizens from States which would not make such information available.

The result: a loss of jobs and security clearances—and thus defense contracts—to residents of States which seek stronger protections against the release of arrest data. In the Commonwealth of Massachusetts, for example, Mr. Cooke stated that thousands of citizens have already been adversely affected because my State refuses to give DOD arrest data. Thus even the person with no arrest record at all suffers because the Defense Department says it cannot complete its investigation without it.

The matter of State regulation of arrest data is, of course, not a two-way street with Mr. Cooke. He believes that State and local governments should be allowed to enact more "liberal" access statutes authorizing the release of arrest data to any person, group, official, or institution they wish. What States could not do, under the DOD proposal, is to pass more stringent regulations.

What does all this signify? It is simply this: that President Nixon and administration officials, while professing to be in favor of protecting privacy, are doing

all they can to scuttle proposals which would secure that basic right. The public disagreements among and contradictory statements by Nixon appointees, such as Mr. Saxbe, Mr. Kelley, and Mr. Cooke, could adversely affect the chances for passage of a strong bill. It leads me to wonder whether Congress and the American people have again been the victims of administration double-dealing.

Mr. RARICK. Mr. Speaker, this Nation's commitment to the principle of the individual's rights to privacy has a long and honored history. Yet the growing invasion of our citizens' privacy by agencies of the Federal, State, and local governments, as well as, by independent agencies and businesses is alarming to Americans.

Dossiers containing information on almost every American citizen are tucked away in computer data banks and files all over the country. A brief list of some of the records and information which may have been collected on each of us is frightening: Adoption, airline flight record, arrests, bank accounts, bank loans, birth, car registrations, census, church records, consumer credit, conviction records, customs, divorce, draft status records, driver's license and record, drug prescriptions, employment, FBI, fingerprints, food stamps, general health, gun registration, ham radio registration, hotel, hopsital, immigration, insurance, job application, library cards, marriage, medicare, medicaid, military, mortgage, newspaper morgue files, passport, pet registration, police, pilot registration, political activity, private investigators records, psychiatric, school security clearance, social security, stocks and bonds transactions, subscription mailing lists, telephone, universities, utilities, voter registration, and welfare.

This is by no means a complete list of the official records maintained on our people. Modern communications and computer techniques place this information within easy access of anyone who wants to obtain it. A centralization of this mass of private and official information has a chilling, intimidating effect on even the most freedom loving, independent citizen.

The celebrated burglary of "Dr. Ellsberg's psychiatrist's office," to illegally obtain the confidential medical records of a dissident political figure, made front page headlines and focused the public's attention on the question of privacy. The "Plumber's Unit" became a household word and trials and convictions followed.

But scant attention has been given to the legalized burglary of confidential medical records by the Professional Standards Review Organizations—PSRO—which became law on January 1, 1974. This radical concept of government intervention into privacy, through computerization of confidential medical records, would accomplish on a nationwide scale what the "Plumbers" failed to do.

I mention PSRO's invasion of individual privacy as an example of how far government snooping into the personal affairs of its citizens can go, with the consent and approval of Congress. Even though it did not intend to allow legalized invasion of doctor's offices and privileged doctor-patient communication and records, the 92d Congress, and many of us here today, passed this law. Authorizing HEW's unelected army of bureaucrats to pry into the medical history of our people.

PSRO was passed in the last minute rush of the 92d Congress, tucked away in the massive Social Security Act as a Senate amendment added in conference. It is so easy for Congress to unwittingly grant authority to the Federal agencies which, under bureaucratic interpretation, infringes on our people's rights.

Professional Standards Review Organizations establish a network of interlocking committees reaching from the offices of local doctors all the way to the Secretary of Health, Education, and Welfare. They are responsible for establishing national standards of diagnosis, treatment and care of medicare and medicaid patients. The medical history of some 50 million patients and 10 million hospital admissions are presently subject to PSRO monitoring.

But this law allows PSRO to monitor, not only medicare and medicaid patients, but it also empowers them to inspect the medical and hospital records of everyone treated by a medical doctor or admitted to a hospital. We are told that this wholesale invasion of confidential medical records is necessary for HEW to establish and computerize national "norms of health care, based on typical patterns of practice." If this must be done, there is no doubt that it cannot be accomplished without resorting to violating the privacy of the poor, the aged, and the sick in this country.

The right of privacy, in the past, sacred in medical relationships, will be violated without benefit of a search warrant, court order, or authorization by the patient. These safeguards of individual liberty will not stand in the way of HEW's PSRO inspectors.

No matter how well-meaning, careful, and trustworthy our HEW officials and employees are, the very compilation and storage of this private information lends itself to fear of abuse. No agency is immune from improper exercise of power, as we have seen in recent years.

If this Federal seizure of medical records sounds farfetched to some of our colleagues, I should like to point out that in my State of Louisiana we have already had an example of this happening. All the admission records of a private psychiatric hospital near New Orleans were demanded and received by HEW last year. This was done without court order or search warrant, and certainly without the knowledge or consent of the individual patients who had sought treatment for mental problems. Do not think that it cannot happen; it is already happening.

Medical records will become public records. The PSRO section of the Social Security Act sets penalties for disclosure of the information collected by the local PSRO's. However, under existing law, not changed by the PSRO section, disclosure of information contained in HEW files can be made in accordance with regulations established by the Secretary. Section 1106, paragraph B, allows the Secretary to honor requests for information:

"If the agency, person or organization making the request agrees to pay for the information and services requested . . ."

Not only is this invasion of privacy, but it is invasion of privacy for a profit.

Professional standards review organizations and the threat they represent to the sense of security and individual control of the private and confidential aspects of our lives, is but one example of the privacy issue we are addressing here today. By our congressional commitment to the Rights of Americans to maintain their privacy from undue government interference, we are opposing this type of legalized surveillance of our people.

Already the medical societies of California, Illinois, Indiana, Kentucky, Louisiana, Maine, Michigan, Nebraska, Nevada, Oklahoma, Texas, and Virginia have approved resolutions seeking repeal of PSRO or opposing any participation in the program.

This question of privacy, and the infringement of that right by government at all levels and by private companies, goes to the very foundations of our constitutional government. It is not merely the loss of medical doctors' right to maintain medical confidentiality, as in the case of PSRO. At stake here is the very question of whether or not in a government of laws rather than of men, laws can be used to restrict the basic liberties as secured under the Constitution.

I am outraged by this participation today, and its show of congressional support for individual freedoms, that we can curb this frightening trend in America today.

Mr. RHODES. Mr. Speaker, the computer era has brought many benefits to our Nation, both in increased business capacity and in our personal lives. Along with the good however, problems have arisen regarding data storage and the availability of information about the private lives of millions of Americans. It is time that we take an in-depth look at what is being done—and take steps now to protect personal privacy in the future.

There are at present, 54 nationwide organizations which have 750 data banks containing extensive information on 130-million citizens. These dossiers are, in too many instances, readily available to persons, business firms, or other agencies. We need to review our policies with regard to both data collection and data availability or dissemination.

In a recent series of articles, the New York Daily News has related some of the personal disasters arising from misuse of private information. While much of this raw data is hearsay, it does give rise to a concern over the potential scope of the underlying problem. One man had his credit ruined and his business reputation shattered by vicious allegations made by a spiteful neighbor during a routine credit organization check. In addition, the man was unable to find out what malicious information was being used against him. As another example, we all recall the celebrated case in which an auto insurance firm refused to renew a policy because they did not like the way the potential buyer kept house.

Like it or not, we have become a nation of snoopers. Data is now collected by various sources and can be collated from these numerous sources and put together into a dossier that represents an overt intrusion into the privacy of individuals. In most cases, the victim is unaware that his neighbors, fellow workers or possibly even his laundry man have been queried about his habits, his occupation or his home.

Privacy is an extremely perishable commodity. It is one of the civil liberties that differentiates life in the United States from that of totalitarian governments, where life belongs to the State. We cannot sit idly by and allow dictatorship by data to gain a foothold in our country.

One alarming aspect of the data decade is the interchange of information. I am told that some State agencies have sold the names of license holders to peddlers of automotive accessories. Supposedly confidential medical records are sometimes exchanged by insurance firms. Credit information is linked into a gigantic nationwide complex. "This personal information may be collected without the consent of the individual; without provision to check its accuracy; and without control over its dissemination." This was the summation of the dangers of today's data crisis by a special Commission on Privacy from the State of Massachusetts.

There are some who now propose that each of our citizens be given an identifying number to wear from the cradle to the grave. We are not machines, we are people. We have a constitutional prerogative of freedom in the pursuit of happiness, and should not have the ominous shadow of the automated data center hanging over us or dictating the terms of our lives. We are already deluged with numbers—from social security and zip codes to telephone numbers that continue to grow in length. We do not need more numbers, but we do need more opportunity to retain human dignity and individual identity.

We must take a firm first step toward heading off 1984. We must remove the Orwellian threat of a helpless citizen enmeshed in the coils of an all powerful punchcard system. A key element of this effort would be a requirement that individuals be given access to information about them which is used. Responsibility must be placed on those collecting and disseminating information to vouch for its accuracy. The misuse of data must be stopped by allowing the individual to ban use of information collected for one purpose to be used for another. We need to review our data collection and dissemination policy now. I believe that H.R. 12574, H.R. 12575, and H.R. 10042 provide an excellent opportunity for beginning this urgent task .

A process that today may produce only the irritation of unwanted junk mail, or pestiferous phone calls on behalf of unneeded products, can speedily develop into a time bomb, ticking away in an individual's data file, which one day can explode with devastating results for his or her future.

Much as I dislike to add more Federal regulations to an ever-increasing pyramid of Federal power, I feel that in this instance we are justified—and obligated—to protect the welfare of our individual citizens from depredations by data, from unscrupulous exploitation of reports on their private lives.

I feel that H.R. 10042 is an important piece of legislation—an 11th precept to the bill of rights. In today's omnivorous computer world, the right of privacy must be protected here in America—the greatest bastion of individual freedom anywhere on Earth.

Mr. LITTON. Mr. Speaker, in recent weeks, President Nixon following the advice of Vice President Ford, revoked a year old Executive order which authorized the U.S. Department of Agriculture to inspect the tax returns of our Nation's 3 million farmers. This Executive order was fraught with abuse since its issuance had opened the door to unwarranted intrusions into the privacy of the American farmer and had established a precedent for future government investigation of the tax returns of entire classes of our citizens.

The fact that this unprecedented Executive order remained in effect for a full year and the fact that by revoking it the administration has in effect admitted its potential for abuse, clearly demonstrates that our tax laws must be changed to see to it that such a dangerous order is never again issued.

Accordingly, last October I introduced H.R. 10977, designed to insure and protect the confidential information that the citizens of this Nation entrust in good faith to their government.

My bill, if enacted, will substantially alter the present treatment of tax returns, making the data contained therein information that is inherently private rather than inherently public.

Under the terms of my bill, now commonly referred to as the "Taxpayer Privacy Act," tax returns will be available for inspection by specified government entites, solely for the legitimate purposes of tax administration and/or law enforcement. This proposal would in no way hinder the Internal Revenue Service or the Department of Justice in the prosecution of tax evasion or tax fraud. Moreover, quick enactment of "The Taxpayer Privacy Act" will insure the confiden-

tial status of tax returns filed by the American taxpayer and will permanently close the door to potentially unlawful invasions of personal privacy.

For well over a year now, I have been doing all that I could to block what I consider an administration scheme to bare information contained in individual Federal tax returns.

On January 18, 1973, President Nixon issued Executive Order 11679 authorizing the Department of Agriculture to inspect income tax returns filed by persons having farming operations. This order applied to returns filed for taxable years beginning on or after January 1, 1967. The President's stated purpose for the order was to allow the Department of Agriculture to obtain data from farm operations for statistical purposes only. It did not indicate specific data to be gathered. On January 23 new Internal Revenue Service regulations went into effect to implement the Executive order.

Neither the Executive order nor IRS regulations limited the type or amount of information that could be released to the Department of Agriculture. The January 23 IRS regulation stated:

"The Secretary of the Treasury, or any officer or employee of the Department of the Treasury with the approval of the Secretary, may furnish the Department of Agriculture (for the purpose of obtaining data as to the farm operations of such persons) with the names, addresses, taxpayer identification numbers, or any other data on such returns or may make the returns available for inspection and the taking of such data as the Secretary of Agriculture may designate."

The President issued a revised Executive Order No. 11709 on March 27, 1973. The revised order permitted Department of Agriculture inspection of farmers' tax returns in accordance with amended IRS regulations. These regulations limited the scope of the data which could be obtained compared with the regulations issued with the prior Executive order. The new regulations provided that only "names, addresses, taxpayer identification numbers, type of farm activity, and one or more measures of size of farm operations such as gross income from farming or gross sales of farm products," would be furnished the Agriculture Department.

In the original Executive Order 11679 any employee of the USDA with permission of the Secretary of Agriculture, was given authority to examine any and all tax returns of citizens showing farm income or expenses as long as they could justify such examinations by saying it was for statistical purposes. The President rescinded his order on March 27 and issued Executive Order 11709. However, under 11709, farmers' tax returns were still potentially an open book. In the revised Executive order, any employee of the USDA with permission of the Secretary of Agriculture had the authority to examine any and all farmers' tax returns and to obtain any piece of information from such tax returns as long as that information can be construed to mean a measure of size of the farming operation of the taxpayer. Close examination of the tax returns will clearly show that almost any piece of information on the return will be considered a measure of the size of the taxpayers' farming operation.

It is very significant to note that these Executive orders were formulated as a model or prototype for future Executive orders opening tax returns for similar statistical uses by other Federal agencies. In response to a congressional inquiry last year, the Justice Department said:

"The original order was prepared by the Department of the Treasury in language designed to serve as a prototype for future tax return inspection orders."

My proposed Taxpayer Privacy Act would prevent Executive orders from ever being used for such unwarranted invasions of privacy.

My proposal explicitly states that all tax returns are confidential and private records and may be opened to inspection only by the following persons at such times and in such manner as the Commissioner of the Internal Revenue Service by regulation prescribes:

First, the taxpayer or his attorney; second, officers and employees of the Internal Revenue Service, the Treasury Department, and the Justice Department for tax administration and economic stabilization purposes; third, shareholders of record owning 1 percent or more of a corporation; fourth, tax officials of the States, the District of Columbia, territories or possessions; fifth; the Ways and Means Committee of the House, Finance Committee of the Senate, and Joint Committee on Internal Revenue Taxation or by other specifically authorized committees of Congress; sixth, the Attorney General, his assistants, and U.S. attorneys in the performance of official duties or for litigation; and seventh, officers and employees of the Executive Department if necessary for legitimate law enforcement purposes.

Last year, several congressional committees held hearings on the confidentiality of Federal tax returns. In particular, these hearings focused on Executive Order 11697 and 11709. As a result of these hearings, the House Committee on Government Operations unanimously recommended that our tax laws be amended "to make tax returns explicitly confidential except as otherwise limited for tax administration, enforcement, and other purposes approved by Congress." The present Commissioner of the Internal Revenue has endorsed this principle of confidentiality. And most recently two of the Nation's leading newspapers in back-to-back editorials have encouraged the Congress to quickly enact, and for the executive branch to endorse, legislation which will insure the confidential status of information contained in citizens' tax returns.

Mr. Speaker, for the Record, I wish to insert an editorial from the March 22, 1974, edition of the Washington Post and a related editorial from the March 4, 1974, edition of the Washington Star-News:

[The editorials follow:]

THE MISUSE OF TAX RETURNS

President Nixon has advanced the cause of personal privacy by revoking the year-old executive order which allowed the Agriculture Department to examine the tax returns of the nation's 3 million farmers. The cancellation, which was recommended by Vice President Ford's new committee on privacy, was long overdue, because the executive order involved should never have been issued at all.

This controversy has been a good example of the way in which bureaucracies, if not carefully watched, can chip away at citizens' rights without meaning to do any damage at all. The order was issued, in essence, because the Agriculture Department wanted to collect a large amount of information on farmers' incomes and decided it would be more convenient to consult the files of IRS than to ask individual farmers to provide the sensitive data directly and voluntarily. But by giving USDA blanket permission to look at the tax returns of a whole class of citizens, President Nixon approved a major departure from past practices, under which agencies had been allowed access to tax returns only when probing some individual's activities.

Executive Order 11697 thus raised serious privacy issues, as Rep. Jerry Litton (D-Mo), Rep. Bill Alexander (D-Ark.) and others protested. The order was doubly troubling because, according to a Justice Department memorandum, it was meant to be a "prototype" for similar broad searches of IRS files by other agencies. Thanks to a House government operations subcommittee probe and the resistance of the IRS, the Agriculture study was never carried out. Now, finally, the entire exercise has been abandoned.

Another case, involving the Office of Education, also suggests that agencies may be getting more sensitive to taxpayer's rights of privacy. This case involves the program of basic educational opportunity grants, aid given to college students from low-income families. Since the grants are based on complicated calculations of need, the program's administrators understandably want to be able to verify the income data which applicants submit. The problem is how this should be done. Last year, the application form included this affidavit:

I (We) certify that I (we) have read this application and that it is accurate and complete to the best of my (our) knowledge. I (We) authorize the United States Commissioner of Education, or his representative, to obtain from the District Director of Internal Revenue with which it was filed, a copy of the 1972 Federal Income Tax Return upon which the computation of expected family contribution is based, in order to verify the foregoing statement. I (We) further agree to provide, if requested, any other documentation necessary to verify information reported on this form.

Thus every applicant, whether or not he could decipher the fine print, was—as the price of the application—allowing the agency to inspect his tax return without further notice. An agency spokesman says that the language was meant primarily as a warning against fraud and that no such searches have actually been made. Indeed, somebody had some second thoughts about the whole procedure, because the language in this year's form is slightly bigger and much better. It reads:

I (We) certify that I (We) have read this application and that it is accurate and complete to the best of my (our) knowledge. I (We) agree to provide, if requested, any documentation, including a copy of my (our) 1973 Federal Income Tax Return, necessary to verify information submitted on this form.

Such changes are encouraging—but the privacy of tax returns should not depend on bureaucratic second thoughts. IRS Commissioner Donald C. Alexander agrees. He has endorsed a House Government Operations Committee recommendation that federal tax returns should be made explicitly confidential by law, with Congress—and only Congress—deciding what exceptions are justifiable in the interests of law enforcement and other public purposes. This is a simple, sensible approach. Vice President Ford's committee should endorse it and Congress should act on it right away.

MISUSE OF TAX RETURNS

There was a time when citizens could assume that, except for examination by Internal Revenue Service agents, their federal income tax returns were reasonably safe from the prying eyes of curiosity seekers and others with more mischievous or malevolent motives.

But it's getting so that congressional committees have little trouble getting returns for investigations of one sort and another, and the forms seem to float hither and yon among officials in the executive branch without much thought to the traditional obligation of confidentiality.

This was dramatically demonstrated the other day in the disclosure of a White House memorandum which said President Nixon suggested in June 1969 that his staff be given access to the returns of former presidents so he could learn what deductions they had taken. While Mr. Nixon has denied seeing the returns and doesn't recall asking aides to obtain them, the memorandum was written by a former aide at a time when Mr. Nixon seemed intent on making use of every loophole available—and some that had been closed off—to lower his tax bill. That such use of tax returns is illegal apparently made little difference to the White House.

That is distressing enough but now we have an even more ominous invasion of the taxpayers right to the privacy of his returns. Only recently some members of Congress discovered that Preident Nixon in early 1973 issued an executive order allowing the Department of Agriculture to examine the tax returns of the nation's three million farmers.

Apparently there was no evil intent in the department's wish to examine the returns. Evidently it wanted to compile statistical information about farmers that might be useful in formulating farm policies. But regardless of the motive, the mass examination of tax returns by any governmental agency not involved in the enforcement of income tax laws is completely unjustified.

We agree with Representative Alexander of Arkansas who saw the presidential order as foreshadowing a "frightening prospect" that other departments and agencies will be given access to personal income information of various classes of people. He raised the possibility, for example, of the Department of Commerce wanting to look at returns from businessmen, the Federal Housing Administration wanting to inspect returns from homeowners, or the Department of Labor wanting to examine returns of union members. Lest anyone think Alexander is far off base, a Justice Department official was quoted as saying that the presidential order was drafted as a model so that tax returns could be used for statistical purposes by other federal agencies.

President Nixon has made a big thing lately of the right to privacy. He also has protested allowing congressional committees investigating Watergate and impeachment to "paw" through White House records on a "fishing expedition." If Mr. Nixon is serious about protecting privacy, he could start with rescinding the order involving farmers' tax returns. Neither the farmer nor any other citizens want Washington bureaucrats pawing through their income tax returns on a fishing or any other kind of expedition.

If the President doesn't rescind the order, the Congress ought to do it through legislation that would prohibit any such flagrant misuse.

At this point I wish to commend those cosponsors of my bill who fought so hard and well to have this unwise order revoked. I especially commend Representative Bill Alexander of Arkansas; Representative Bill Moorhead of Pennsylvania; Senator Lloyd Bentsen of Texas; Mr. Norman Cornish of the House Government Operations Committee; and a first-rate journalist, Mr. Alan Emory, of the Watertown, N.Y., Daily Times. Their efforts on behalf of the public's right of privacy is one of the brighter aspects of an otherwise depressing drama that has unfolded before us during the past year.

Also, I feel that the President's decision to revoke Executive Order 11697 is an excellent step in the right direction, reflecting his recognition that the original order was, in fact, a serious mistake. At the same time, I am deeply concerned that this situation may recur in one form or another, particularly in light of the 1973 Justice Department opinion suggesting that the order now rescinded serve as a "prototype" for all other Federal agencies. The Taxpayer Privacy Act is intended as a safeguard to provide assurance that this kind of potential abuse will not recur, and will not serve as a "prototype."

Mr. Speaker, the excesses of a government pose threats to the basic rights of the governed. While the revocation of Executive Order 11709 was an admirable response to outraged protest, the American people deserve the full protection afforded by my bill, H.R. 10977, and by S. 3238, introduced by Mr. Bentsen, the distinguished Senator from Texas.

I urge my colleagues—in both Houses of the Congress—to support these efforts to protect the precious right of privacy of the American people, a right whose circumvention or outright breaching can lead to an ever growing assault upon those other rights that also are vital and indispensable parts of our American heritage.

Mr. TIERNAN. Mr. Speaker, much attention has been focused on the Government intervention into our privacy. Wiretaps and eavesdropping devices often violate the citizen's fundamental rights to privacy. It is very important to protect these rights but there is one area where privacy works a true hardship on the American citizen. This is the field of corporate privacy. Corporations often have tight disclosure policies. By keeping private most of their activities, the possibility of fraud is greatly heightened. One example of the magnitude of fraud that can be perpetrated is the Equity Funding case. I would like to enclose an article from the Wall Street Journal on Equity Funding. This article highlights the hardships that can be caused when a corporation is capable of keeping their records secret from the investing public.

[The article follows:]

[From the Wall Street Journal, Mar. 29, 1974]

MANY PEOPLE'S DREAMS CAME CRASHING DOWN WITH EQUITY FUNDING

(By William E. Blundell)

"Every day I wake up and wonder what will happen to me," says Peggy Rahn, a 74-year-old widow living in a small New York apartment. Her bankbook says she has $900 left in the world. Her Social Security payments don't quite match her rent. After working for 55 years and always being self-sufficient, she is being inexorably pushed toward the welfare rolls. She wishes she had never heard of Equity Funding Corp. of America, in which she invested $7,000.

Across the Hudson River in New Jersey is a man who is keeping a terrible secret. In failing health, he yearns for retirement but still drags himself to work. His worried wife and son don't understand why. Self-employed, without any Social Security benefits coming, he cannot bear to tell them that most of what he has saved over the years now is so much wallpaper. He put the money, more than $25,000, into the 9½% bonds of Equity Funding.

In a town in Nebraska, a college student needed medical attention his family couldn't afford. They borrowed on their assets so he could make a surefire investment that would pay the doctor bills. The investment was the common stock of Equity Funding. His treatments have been delayed, and his father and mother try not to let him see how hard-pressed they are.

These are only a few of the lives touched by the Equity Funding scandal, one of the biggest and most audacious securities frauds in history. Today, almost a year to the day since an astonished public learned that Equity Funding was a house of cards, countless thousands of people continue to pay a price for the manipulations of a few. One figure tells part of the story. At the beginning of 1973, before word of bogus insurance and inflated assets at Equity Funding went whispering down the canyons of Wall Street, the company's common stock had a market value of about $288 million. Today it is worth nothing. So are the company's bonds and warrants.

WHAT IT MEANS

This, of course, does not mean that securities holders should throw all their certificates away. Equity Funding now is being reorganized under Chapter 10

bankruptcy proceedings, and it is expected to emerge as a new company that will issue new securities to satisfy claims of defrauded investors. But trustee Robert Loeffler warns that the new stock, at first anyway, would be worth only a tiny fraction of the price the market placed on Equity Funding securities before the scandal broke. "There just isn't enough in the company to support that kind of value," he says flatly.

The potential losses from Equity Funding mean most to small investors—the butchers and bakers and candlestick makers who risked sizable percentages of their savings. For them, Equity Funding means a pinched household budget, a vacation untaken, a new home still a dream, wearing old clothes because they can't buy new ones, or a blighted retirement. There is much bitterness.

"Where were the men who were supposed to watch out for us little people?" asks a Long Island resident whom we will call Larry. "They tell you it's all safe, all regulated, so they can get you to invest. Then you find out it's still nothing but a big crapshoot, and you're marked for a loser. Would you ever believe an insurance company that size going bust? Aren't they supposed to be like the Rock of Gibraltar?"

"DON'T WORRY"

Larry, who is retired, put $21,000 in Equity Funding bonds. When the company's securities plunged in value upon rumors of fraud, Larry called his broker. "He said, 'Don't worry; even if they stole $20 million, the company has more than a hundred million in assets,'" Larry recalls. Now Larry and his wife no longer can take their usual vacation in Florida or anywhere else, she isn't buying any new dresses, and the two are struggling just to meet household expenses.

Larry's fellow victims are a diverse lot, including eight members of the Bruni family in Havertown, Pa., who belong to an investment club with $2,000 in Equity Funding; teachers in Ohio; the present and future student bodies of Princeton, Amherst, Williams, Sarah Lawrence and sundry other schools; children in Pittsburgh with learning disabilities; the innocent employes of Equity Funding itself, and at least one reporter for this newspaper, who bought $3,000 of the 9½% bonds "just to get better interest on my money than in a bank."

To those hardest hit, the potential financial damage is often compounded by pervading despair. One 30-year-old bachelor from Sherman Oaks, Calif., a small-business man with most of his savings tied up in $22,500 of Equity Funding securities, says: "I've had to pound and grind to make that. I can't count the nights I've sat up sighing and saying to myself, "Everything you worked for for years is gone.'"

The bachelor businessman also developed a bizarre physical reaction. After morbidly brooding over every word written in this newspaper about Equity Funding in the first few days after the swindle had been exposed, he found himself getting stomach pains at the very sight of The Wall Street Journal and had to stop reading it altogether for a while. But another victim, Lydia Bowne, says that the "whole thing was like a novel, fascinating," and has a scrapbook several inches thick filled with clippings. An employee of Bankers National Life, and Equity Funding subsidiary based in Parsippany, N.J., Miss Bowne wound up with 500 shares of Equity Funding exchanged for her good stock in Bankers National when the two firms merged.

To others, the strain of keeping their losses secret from friends and family is nearly unbearable. "I don't know how much longer I can do it, but I have to," says one man who invested for retirement. "How can I tell my wife I lost most of the money we were going to retire on? I don't know what it would do to her, and I'd die of shame."

Larry, the Long Island resident, and his wife fear loss of status if their friends learn that they now are strapped. "Nobody knows the trouble we're having. Nobody can," he declares. "My wife would commit suicide or something."

A special place in the ranks of the fraud victims belongs to those unfortunates who bought just before trading was halted. The student in Nebraska bought 500 shares just minutes before the New York Stock Exchange halted trading in the common stock March 27 of last year. An hour or so before, a law student from Brooklyn, Lloyd Somer, put the money he had earned from his job the previous summer into 100 shares. "I know you take a risk whenever you invest, but I certainly didn't expect to blow the whole bundle in one morning," Mr. Somer says. He isn't in the market anymore.

BUYING IN IGNORANCE

Diverse as they are, many victims have one thing in common. They bought Equity Funding in ignorance, relying on casual tips from friends and brokers and not doing much homework on the company themselves. Peggy Rahn, the 74-year-old New York widow, says she bought because she once worked for a man who was a friend of Michael Riordan, a former Equity Funding chief executive who died in a mud slide in 1969. Numerous bondholders bought under the mistaken belief that the bonds were of top-grade investment quality.

But given the nature of the fraud, in which audited financial statements turned out to be figments of the imagination, homework probably wouldn't have made most potential investors overly suspicious anyway. One who did study the company, did attend annual meetings and was still taken is Carl McWade, a semiretired market-research specialist in Los Angeles.

"I met some of those guys" (the company's top executives) at the 1972 annual meeting," he says, "and they looked fine to me—clean-shaven, clean shirts, nicely dressed. They certainly didn't look like crooks, and there wasn't any reason to think anything was wrong."

In early 1973, however, his stock, purchased at more than $42 a share, fell to $27. Deciding that it was time to get some first-hand information, Mr. McWade called Samuel Lowell, then executive vice president of Equity Funding. Just general market conditions, Mr. McWade recalls Mr. Lowell as having said. The stock went to $21, and Mr. McWade picked up the phone again.

He says that this time Mr. Lowell said he suspected that someone was conducting a bear raid on Equity Funding and that company executives were urging "our friends back East" to buy the stock, which he expected to soar to $70. Reassured, Mr. McWade held on. A few days later, trading was halted, and the scandal was made public. Mr. Lowell now is under federal indictment with 21 other defendants in the Equity Funding case.

HOW THE FUNDS WERE AFFECTED

Individuals who invested directly in Equity Funding represent only a fraction of those affected by the fraud. Tens of thousands of others, most of whom don't even realize it, are also victims. They are the ultimate beneficiaries of various trusts, pension funds and endowments stuck with Equity Funding securities.

To the men overseeing these large diversified funds, the Equity Funding debacle is only a minor setback, not unexpected in an era when money managers are investing in speculative stocks and bonds for growth and higher income, and not just in blue chips for safety. "If you bought nothing but the AT&Ts of the world, you'd get nothing but an AT&T return, and that isn't good enough. You can't achieve the overall results we've achieved without taking some risks," says Paul Firstenberg, financial vice president of Princeton University.

If the $500 million Princeton Endowment Fund has to take a loss on the $1.3 million it has invested in Equity Funding, it will be barely noticeable. Neither would a $10.8 million loss on its Equity Funding securities mean much, relatively speaking, to the State Teachers Retirement System of Ohio, which has $2.6 billion in assets. Nor would a $50,000 loss to the trust providing income for the Laughlin Children's Center in Pittsburgh, which treats youngsters with learning disabilities.

That's one way of looking at it. But the fact remains that to the extent that these investments are losses, the beneficiaries of these funds will be the poorer. For example, $50,000 covers a third of the annual operating budget of the children's center. At the colleges holding Equity Funding, the potential loss can be translated into salaries for professors and scholarships for students.

EQUITY'S EMPLOYEE

As a class, probably no group has suffered as much as the present and former employes of Equity Funding who were innocent of any wrong doing. While the fraud was going on under their noses, they bought heavily in their company's stock, borrowed on it in some cases, and put their friends and relatives into it.

Larry Williams, an attorney and chief of compliance at Equity Funding, believed his bosses when the rumors flew and the stock fell; he urged his brother, who manages their father's affairs, to invest. On Monday, March 26, he did, buying $10,000 of stock for the senior Mr. Williams. The next day trading was

stopped. "Stanley Goldblum (the former chairman and president) assured me—he swore up and down—that there was nothing, absolutely nothing, wrong," Mr. Williams says. "God, what a fool's paradise I was living in."

Then there are all the Equity Funding employes who had to be let go during the past year because there wasn't any work left for them. "People above the clerical level have had a terrible time getting new jobs," says Mr. Loeffler, the trustee, who tries to help them. "It's nothing personal, nothing to do with the employe himself. It's just that no company seems to want a personnel file in its records with the words 'Equity Funding' in it."

Mr. LONG of Maryland. Mr. Speaker, on July 30, 1973, I introduced the first bill to stop the then recently revealed White House practice of recording the conversations of important officials in the Government, diplomats, and even White House staff members—without their knowledge. My "no recording without notification" bill, H.R. 9667, would effectively plug the loophole in the 1968 Omnibus Crime Control and Safe Streets Act which now allows secret taping not only in the White House, but anywhere so long as merely one of the participants knows. Under that statute, if "A" and "B" are conversing, "A" could secretly records the conversation without "B's" knowledge—no law would be broken. Under my bill, all parties to a communication must be notified before the conversation may be recorded legally.

The courts would, of course, retain the power to authorize wiretaps for investigations of criminal or espionage activities; H.R. 9667 would simply stop the type of secret bugging which, as pointed out by one U.S. district court judge, has been allowed "to proliferate without judicial supervision."

The "no" recording without notification" bill has been cosponsored by 27 Members of Congress. And President Nixon's most recent state of the Union message recognized the need for various legislative proposals to protect the individual's rights to privacy. The President added:

"And I look forward again to working with this Congress in establishing a new set of standards that respect the legitimate needs of society, but that also recognize personal privacy as a cardinal principle of American liberty."

I feel confident the majority of Americans would support the objectives of H.R. 9667, and I hope for its early passage by this session of Congress.

Mr. RODINO. Mr. Speaker, I certainly commend our distinguished colleagues who have sponsored this special order on the congressional commitment to privacy.

We in America are now struggling to find a solution to reestablish the rights of personal privacy in the computer age. I am particularly pleased that my Judiciary Committee's Subcommittee on Civil Rights and Constitutional Rights is actively working on various proposals designed to help strike that delicate balance between the legitimate needs of law enforcement for information which is protective of the public welfare and that most prized but elusive civil liberty of the individual right to privacy.

It is encouraging to realize that we are not alone in this effort. As a delegate to the NATO North Atlantic Assembly for some years, I am very aware that our country is but one of a host of nations facing this challenge. We can certainly benefit by considering the work already done, and the conclusions thus far reached, of the other advanced nations of the world.

Mr. Speaker, I think it is highly significant that the Council of Europe—representing 17 European countries—has been preparing a policy on individual privacy vis-a-vis electronic data banks in the private sector for 3 years. In September, 1973, the Council's Committee of Ministers adopted a resolution on this issue. I believe the Congress should carefully study the succinct and realistic statement of 10 principles of privacy over information collection, maintenance, use and dissemination that these 17 nations have together been able to develop. It bears the mark of people sensitive to their liberties in a fast-moving, technological age. I include what can well be termed the Council of Europe's "Ten Commandments on Information Privacy" herein.

[The information follows]

[Council of Europe, Committee of Ministers]

Resolution (73) 22—On the Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector

(Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies)

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve a greater unity between its member States;

Conscious of the already widespread and constantly increasing use of electronic data processing systems for records of personal data on individuals;

Recognising that, in order to prevent abuses in the storing, processing and dissemination of personal information by means of electronic data banks in the private sector, legislative measures may have to be taken in order to protect individuals;

Considering that it is urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergencies between the laws of member States in this field;

Having regard to Resolution No. 3 on the protection of privacy in view of the increasing compilation of personal data into computers, adopted by the seventh Conference of European Ministers of Justice,

Recommends the governments of member States:

(a) to take all steps which they consider necessary to give effect to the principles set out in the Annex to this resolution;

(b) to inform the Secretary General of the Council of Europe, in due course, of any action taken in this field.

ANNEX

The following principles apply to personal information stored in electronic data banks in the private sector.

For the purposes of this resolution, the term "personal information" means information relating to individuals (physical persons), and the term "electronic data bank" means any electronic data processing system which is used to handle personal information and to dessiminate such information.

(1) The information stored should be accurate and should be kept up to date.

In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

(2) The information should be appropriate and relevant with regard to the purpose for which it has been stored.

(3) The information should not be obtained by fraudulent or unfair means.

(4) Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

(5) Without appropriate authorization, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

(6) As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

(7) Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

(8) Precautions should be taken against any abuse or misuse of information.

Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.

(9) Access to the information stored should be confined to persons who have a valid to know it.

The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

(10) Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.

Mr. ADDABBO. Mr. Speaker, I rise to join my colleagues in discussing the congressional commitment to privacy, a subject which is timely and basic to the preservation of our system of government. The President of the United States recently addressed the Nation on the subject of privacy and many Members of Congress have addressed this subject in recent months.

The increasing concern about the right of privacy in the United States is understandable in light of the growth of Government agencies at the Federal, State, and local level and the staggering volume of records maintained by those agencies. The potential abuse of power inherent in this process was illustrated by the activities and proposed activities of those involved in the Watergate scandals.

The list of issues related to the question of privacy is a long one, making it even more difficult to find solutions to the problems in protecting the public from abuses. These issues include assuring access to individuals whose records are maintained by Government agencies, assuring confidentiality of Internal Revenue returns, controlling the disclosure of information by financial institutions, limiting the sale of mailing lists and other lists by private companies, and the growth of computers and data banks as potential invaders of privacy.

Several bills have been introduced in the Congress on each of these subjects and many other related issues. These bills are pending before several congressional committees. The President has made an effort to coordinate activities in the field by directing the Domestic Council to recommend appropriate action.

Because the protection of individual privacy is so basic an element of a free society, this effort requires a bipartisan approach and that is why the administration and the Congress must work together to find effective means to protect the individual against invasions of privacy.

The restoration of public confidence rests in large part on our ability to guarantee fairness and respect for the rights of the individual in Government's relationships with the public. The multifaceted subject of privacy requires our attention now and our action as soon as possible. The records maintained by Government agencies must become models for private business so that Government can regulate where necessary the growth of data banks in the private sector. This can only be done if Government sets an example of fairness in assuring that records are kept to a minimum and where kept they are verified by, assuring access to individuals involved and by effectively barring access to others.

Congressional interest in this issue is evident by the participation by House Members in this discussion today. The extent of congressional commitment to privacy must be illustrated by affirmative action in the weeks and months ahead to protect the individual from abuse and potential abuse of the right to privacy.

Mr. COTTER. Mr. Speaker, I am pleased to join the discussion on privacy which was organized by Congressman Moorhead, Koch, and Edwards. Today our country faces the prospect of a major issue being resolved through nondecision. Will we allow the inertia of technological advance and Government bureaucracy to encroach on the individual American's right to privacy? I believe we cannot afford to let our chance to preserve privacy pass by without effective action on the part of Congress. The courts cannot take the sweeping affirmative action needed to safeguard privacy, and our Executive has conducted itself in such a way as to intrude on, rather than protect these rights. While it was rather strange to hear the President call for legislation on privacy given the administration's track record, nevertheless I applaud this initiative.

Almost every time an American citizen applies for an automobile license, a checking account, a credit card, or one of a hundred similar items, his name and some personal information wind up in a file cabinet or a data bank belonging to a private business or the Government. It seems fair that everyone should be assured that this information would be used only for the intended purpose and seen only by those who receive the information from the individual. And yet the American consumer cannot today be safely assured of this degree of privacy.

Not only does this personal information float around to other businesses or agencies, it often gets used for many purposes other than the original intent of the individual. What is most appalling is that access to these files is open to almost everyone except the person who is the subject of the file.

The Federal Government alone controls over 800 personal data systems under 50 different agencies. By the end of 1975, private businesses will have over 250,000 computers with some 800,000 remote data terminals in operation.

Congress must commit itself now to halt the conscious or unconscious attack of the "computer era" on the individual's right to protect personal information as private information. I have long supported stricter control of Federal files which contain personal information. I am a cosponsor of a bill to create a Select Committee on Privacy and of the Right to Financial Privacy Act of 1973. Enactment of this legislation would be a step toward protecting our rights to privacy. It is time for all of us to make a conscious decision on this problem, rather than let unthinking technological inertia bring us to a world of no privacy, a world not of our own choosing.

Mr. KYROS. Mr. Speaker, I am proud to join distinguished House Members on both sides of the aisle in calling attention to the right of privacy by means of this special order. Not only is this a timely issue, it is also a fundamental and basic one to all Americans.

At this time, Mr. Speaker, it would perhaps be most helpful for me to call the attention of my colleagues to an outstanding article which appeared last year in the Federal Communications Bar Journal. Written by Jeremiah Courtney, this lengthy and exhaustive study discusses the effects of electronic eavesdropping and wiretapping on American life. I commended my colleagues' attention to this excellent history and outline of this major national problem, but because of its length, I include only its conclusion in the record at this point:

[The information follows:]

ELECTRONIC EAVESDROPPING, WIRETAPPING AND YOUR RIGHT TO PRIVACY

(By Jeremiah Courtney)

CONCLUSION

Today's right to privacy is the culmination of a legal metamorphosis, accomplished after decades of painstaking, laborious legal creativity. Originally conceived as a guardian of property, the right to privacy has now emerged as a panoply over the privacy of the person. The result is that all Americans are guarded by a "zone of privacy" that follows them continuously throughout their day-to-day trip through life. One's zone of privacy may contract or expand to fit the particular circumstances, but it is always present to at least a limited extent. The right to private communications is simply one of the facets of the individual's right to privacy, a segment of the legal wall defining a person's zone of privacy.

The right to privacy holds tenaciously to life. It is a vulnerable right, constantly imperiled by the forces of our crowded, technological society. Yet, the right to privacy is essential to the American way of life, for it helps to prevent the individual from being transformed into an Orwellian robot whose life is incessantly monitored so that he will function in conformance with the demands of an impersonal society.

If the fragile right to privacy is to exist, it must be defended zealously. It will require a particular and continuing sensitivity on the part of the FCC Commissioners to every threat to the privacy of communications. It will also require that each and every one of us will have to resist the temptation to use the surveillance weapons that modern technology has bestowed upon us. Finally, we can no longer react apathetically to disclosures of illegal surveillance, as the general public has in the Watergate Caper and as the FCC did when its Wiretapping Caper became the subject of Congressional inquiry. For each intrusion into privacy pushes us that much closer to tyranny.

SUMMARY

The following summary is included, at the usual risks of oversimplification, as an aid to those who desire a quick reference guide to the laws that shield us all from electronic surveillance.

1. All Americans have a right to privacy—"the right to be left alone." The right to privacy emanates from the guarantees in the Bill of Rights, particularly the Fourth Amendment prohibition against unreasonable search and seizure.

2. The Fourth Amendment's warrant requirement governs not only the seizure of tangible items but extends as well to the seizure of words or conversations

by wiretapping or electronics eavesdropping. The Fourth Amendment protects people rather than places. It stands as a safeguard against governmental intrusion into any area where a person has a justifiable expectation of privacy.

3. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520, imposes an overall ban on wiretapping and electronic eavesdropping. It prohibits the interception, use of disclosure of any *wire* or *oral* communication, as well as the manufacturing and sale of snooping devices.

4. Title III permits federal and state governments, after court authorization, to wiretap and eavesdrop to facilitate the investigation of a wide range of crimes. However, the police do not need permission to utilize electronic surveillance in certain emergency situations. The federal law also does not limit the President's power to authorize the use of electronic surveillance to protect the national emergency.

5. Failure to comply with the Federal law subjects the interceptor to stiff criminal and civil penalties. No evidence obtained through illegal surveillance is admissible as evidence in any court in this country.

6. Neither Title III nor the Constitution, as presently interpreted, protect oral or wire communications from interception when it is accomplished with the consent of one of the parties to the communication. This fosters participant or consensual monitoring, whereby one party has the power to make public as ostensibly private conversation. This has led to practices such as the recording of conversations without the knowledge or consent of the other parties. Such practices have a stultifying effect on the justifiable expectation of privacy standard and, if prevalent, can destroy the spontaneity of informal conversations. Title III prohibits this practice only when done for criminal or tortuous purposes.

7. Officers, employees and agents of any communications common carrier, whose facilities are used in the transmission of wire communications, can intercept such communications in the court of its normal rendition of service or to protect its property. Random monitoring is permissible only to conduct quality control checks. The common carrier may not monitor employee calls for such unrelated purposes as establishing that only authorized calls are made by its employees.

8. Federal law allows the Federal Communications Commission to intercept, use or divulge wire or oral communications in the normal course of its monitoring responsibilities to enforce the Communications Act of 1934.

9. Section 605 of the Communications Act of 1934, long the sole federal protector of privacy, now applies only to radio communications. The privacy of radio communications is protected to a limited extent by the Section's prohibition against interception and divulgence of such communications. Interception and disclosure of a radio communication can be accomplished only upon authorization by the sender. The prohibition of Section 605 does not apply to public broadcasting, communications transmitted for the use of the general public, or to those communications relating to ships in distress. Violations are punished by fine and imprisonment.

10. Interception results when any person listens to a radio transmission when this person is not a party to the communication or is not in the presence of one who is a party. A violation of Section 605 occurs whenever a non-party uses information he heard over the radio for his own benefit or discloses such information to any other person without the consent of the sender.

11. The FCC may intercept radio calls and use the information obtained for the purpose of enforcing the Communications Act of 1934 and the Commission's Rules, but not for general crime detection purposes.

12. The FCC permits the use of mechanical recording devices to record telephone conversations as long as the use is identified by a "beep" on interstate telephone calls.

13. The Commission's Rules prohibit the use of any radio device, required to be licensed, for the purposes of eavesdropping without the consent of *all* the parties to the particular conversation.

14. Monitoring a shared radio channel, for the purpose of effective shared use, does not appear to be a violation of Section 605. However, it would be a violation of Section 605 to divulge either the existence or contents of the monitored conversations to any person without the consent of the sender. This may include the act of reporting the improper use of a shared radio channel to the FCC.

Mr. WHITE. Mr. Speaker, I would like to begin my remarks by commending the gentleman from California for his efforts to secure Members an opportunity to speak out on this most important issue of privacy. Individual privacy is a time-

honored and sacred institution in this country. If it is to survive in an era of ever expanding computer technology, we must take steps to insure that frivolous and unreasonable demands for personal information are not placed upon individuals by private institutions and governments. Efforts must likewise be made to make certain that personal data, once collected, are used only for legitimate purposes made known to the individual at the time such data is furnished.

Proponents of individual privacy will be glad to know that the Subcommittee on Census and Statistics, of which I am chairman, has begun an in-depth study of laws and regulations relating to the confidentiality of statistical data collected by various Government agencies, with a view toward ascertaining whether such laws and regulations adequately protect individual privacy. Initial efforts in this study are being directed toward developing a compendium of existing confidentiality rules and regulations—something which does not exist at present. We intend to make this compendium available in the form of a House report. Should study of the compendium indicate a need for hearings and/or legislation, I shall not hesitate to take the appropriate action.

It is my sincere hope that this effort will serve to assure that personal information located in Government files will not be misused.

Mr. PODELL. Mr. Speaker, I am pleased to be participating in this special order. The question of privacy is one of great importance to me, not only as a legislator, speaking for my constituents, but as an individual trying to make a secure life for myself and my family. I am not for a moment deluded by the thought that I, simply because I am a Member of this distinguished body, am therefore protected from abuses of my privacy. On the contrary, it is because I hold the position in life that I do, that I know how very vulnerable this precious right is to abuse and infringement by both the Government and private industry.

I could no doubt tell you any number of horror stories about men and women whose lives were ruined by errors in reporting their past histories by firms specializing in such work. It is most difficult to accept the need for these firms in a complicated industrial society that runs on credit, because many of these firms abuse their privileges.

True, we must know if a person is credit worthy, if he can pay his bills and if he is making enough money to meet his mortgage payments. But do we really have to know about his living habits, or whether he can get along with his neighbors, or even what brand of cigarettes he smokes? What does any of this have to do with being credit worthy?

The problem is one that grows each time you write a check or use your credit card. Banks are now required to keep records of each and every transaction you make, and the Federal Government has access to these records without you ever knowing about it. This is a law that we passed not too long ago, and which the President signed, and which the Supreme Court of the United States upheld only yesterday.

Surely this violates our privacy in conducting our own business transactions, but the Supreme Court does not think so, and there is no provision in the law for protecting your right to the privacy of your own bank records.

If you belong to the Book-of-the-Month Club or hold a Bank Americard, you have unwittingly made yourself eligible for the honor of receiving hundreds of pieces of unwanted mail every year—junk mail. Your name and address have been bartered and sold, like common merchandise, to direct mail advertising companies, and you get nothing from it but higher postal rates and an invasion of your personal privacy.

Your life could be ruined, absolutely and beyond repair, by a faulty report by a firm such as Retail Credit Bureau of America, which is under no obligation whatsoever to make sure that the data it has on you in its dossier—and you can be sure that this firm, or another one just like it, does have a dossier on you—is correct or up to date.

True, you have the right to request to see your record, but in getting your record you are put into a double blind situation. You must supply the company you are seeking disclosure from with your name, address, social security number, current address, past addresses for the last 5 years, and with similar information for your spouse. If they did not have much information on you before you made the request, simply by the act of making the request they will have enough to complete the rape of your privacy.

There is a distressing trend in this country to forming data banks. Such banks already exist for medical information, and are being formed for information on criminal records. These banks are being formed right now, and so far there is no

way of controlling their formation or regulating their use. There is no way of making sure that they will not be subject to abuse, and there is no way of requiring them to be accurate in their information.

In short, we are silently looking on as institutions are being set up which will throw a shadow of big brother over the land.

Privacy is a precious right, and as such must be guarded diligently. We can never be too secure in our right to privacy, and there can never be too many laws enforcing our security in this right. The great misfortune of our society is that there are not enough such laws, and as a result, the average citizen, the consumer, the wage-earner, is at the mercy of big Government and big business. They know more about him and his family than he may know himself, and everything they know can and will be used against him. They are under no obligation to make sure their information is correct, nor are they under any obligation to inform the persons involved that they are part of a statistic in a data bank, or a file in a credit bureau.

The Federal Government seems to be running to excess in ways to invade our personal privacy, and the Supreme Court does not seem to be ready or willing to curb this distressing tread. The President's Commission in Privacy is a step in the right direction, but it will be a long time before that Commission produces any concrete results, and I fear that the President will ignore the recommendations of this Commission as he has the recommendations of so many other commissions set up by him in the past.

Therefore it comes down to the Congress. The responsibility is ours. If we do not take positive action, and take it immediately, to safeguard the right of each and every citizen to be secure in the privacy of his home, and in his business transactions, there will be no right of privacy left for us to safeguard.

I am taking this opportunity to introduce a piece of legislation which I hope will serve to curb some of the abuses we have been discussing here today. It is a bill designed to control the sale of names and addresses to companies that compile mailing lists for the purpose of direct mail advertising.

It requires the written permission of any individual whose name and address is sold for use on such a list. This will be one among many bills designed to increase the degree of privacy we now enjoy, and I feel that this is an essential element in safeguarding that right. For if our right to control the use of our names and addresses is taken away from us, how can we ever be secure in our God-given right to personal privacy?

Mr. CHARLES H. WILSON of California. Mr. Speaker, I am pleased to participate today in the special order requested by the gentleman from New York (Mr. Koon) on the subject of privacy. On December 13th of last year, I spoke in support of House Resolution 633 to establish a Select Committee on Privacy. However this jurisdictional matter is settled, whether by Select Committee or Subcommittee, I must stress the need for Congress to fully evaluate the effects of technology on the operations of government, on the democratic institutions and processes basic to the United States, and on the basic human rights of all our citizens. While technology is advancing at an unparalleled rate and influencing every aspect of American life. I feel that Congress has not taken the time to first understand and then to possibly set legislative guidelines controlling such applications of technology.

I might add that it is indeed ironic that the Nixon administration which has seen no need for an investigation of the U.S. citizen's right to privacy, now embraces this particular issue—perhaps 5 years too late.

During the previous Congress, I had the honor to chair the Census and Statistics Subcommittee of the House Post Office and Civil Service Committee. Our subcommittee explored in great deal the methods and procedures used by the Census Bureau in taking the 1970 Census. We were particularly concerned about the plethora of detailed questionnaires from the Census Bureau and other departments and agencies of the Federal Government which our citizens are required to answer. While I recognize the real need by the Government to obtain this data which will help to justify, continue, and support programs that benefit the entire community, it is doubly important to ensure that people's privacy is protected so that they do not rebel against the information gathering process and refuse to cooperate in future censuses and questionnaires.

I have therefore introduced H.R. 7762, which would amend title 13, United States Code, to assure confidentiality of information furnished in response to questionnaires and inquiries by the Census Bureau. This bill was reported out of the House Post Office and Civil Service Committee on June 4th, and has been

placed on the Union Calendar. The bill would also extend the responsibilities for confidentiality to all officers and employees of the Federal Government. H.R. 7762 is identical to a bill I introduced in the 92d Congress, and during the hearings which I chaired, it was shown time and time again by hundreds of concerned and sometimes irate citizens who communicated with us that they were anxious indeed about the preservation and protection of their personal privacy. But they were only a small sample of a much larger number of Americans who are similarly situated and similarly motivated. Recent surveys had demonstrated to the satisfaction of the subcommittee that an overwhelming number of U.S. citizens feared the regulation of their lives by computers and ancillary electronic hardware.

I believe that there is a profound need for all-encompassing review and recommendations for control of Federal prying and snooping into the private lives of American citizens. Recent abuses by Government prosecutors in the Ellsberg case are perhaps a classical case of the individual's personal rights being violated by an overzealous, all-powerful, and in this case, unlawful bureaucracy.

Mr. Speaker, the time has come for the Congress to legislate greater safeguards to protect the American's essential right to privacy. For, as perhaps the most astute of the framers of our Constitution, James Madison, warned us:

"I believe there are more instances of the abridgement of the freedom of the people by gradual and silent encroachment of those in power than by violent and sudden usurpations."

Mr. HUNGATE. Mr. Speaker, I am pleased to be able to speak today on an issue which reaches to the very fibers of our democratic system—the right to privacy. This right is both one of the most important and most pervasive rights of the citizen, and it is a right very often easily overlooked by a government pursuing one mission or another. Custody of the individual's information resources now seems to be in the hands of unseen and unknown administrators, bureaucrats, and computer operators.

The issue of privacy has been in the forefront of governmental activity for almost three decades now. Concern for individual privacy has long existed in Missouri. In 1959, Senator Tom Hennings of Missouri held hearings on the encroachment of the Federal Government into the privacy of its citizens, which stated:

"Anybody who uses a telephone does so at his own risk and in effect, anyone who engages in conversation surrenders his right of privacy to anyone else who manages to overhear what he says . . . This probably is sound legal doctrine in any police state . . . but neither the United States nor any of the sovereign States have yet gone totalitarian."

In 1968, his successor in the Senate, Edward V. Long, commented:

"The right of privacy encompasses the freedom of the individual to share or withhold from others, according to his own selection, his thoughts, his beliefs, his emotions, his actions, and his past. It is an affirmative claim to human dignity—a claim to an inviolate personality."

His successor, Senator Tom Eagleton, has a distinguished record on behalf of individual liberties, and protection of their necessary adjunct, a free press. Last year, 1973, he introduced the News Source Protection Act, which would assert "The privilege against compulsory disclosure of sources of confidential information is not so much a privilege for the press as it is a privilege for the public."

In 1970, many people were referring to the U.S. Census as the "1970 inquisition." A concerned Missouri citizen wrote to Senator Ervin concerning the census:

"In a true Republic such delving into private lives would not even be considered . . . Our hope lies with a few men of common sense, such as yourself, and the overwhelming desire of the majority of the citizenry for a return to the precepts of our founding fathers."

It is high time legislation is enacted to begin to guarantee the right of privacy as it rightfully should be. When the next census is taken, for example, we should be interested in counting people and not toilets and televisions.

Recognizing the need of a government for information does not recognize a governmental right willfully and randomly to invade one's privacy and then treat such information as another computer file. On February 19, 1974, I was more than happy to cosponsor H.R. 13880, introduced by our distinguished colleague, Ed Koch. There has perhaps not been a better time in our history to begin to reassert our system's values and to once again guarantee protection for those "unalienable rights" we often treat as mere rhetoric.

Mr. BAUMAN. Mr. Speaker, much is said and written about privacy and the degree to which it is abridged in this day and age. But too little attention is given

to the root cause of the loss of so much of our individual privacy; the inexorable expansion of Federal agencies and bureaucracy.

From the Census Bureau to the Federal Home Loan Bank Board, in scores of Federal agencies and bureaus, the amount and type of personal, private information which is required of an individual by the government is enormous. Many of you will recall a controversy several years ago when the Census Bureau sent out forms to thousands of citizens across the country requiring them to inform the Federal Government, under penalty of law, about how many toilets they had in their homes, and whether they were indoor or outdoor. Many more serious disclosures of personal, private information are required of our citizens daily by Federal edict.

A great deal of legislation has been introduced in the Congress which attempts to minimize the invasions of privacy which these Federal agency requirements produce. But while I would certainly endorse many of these efforts, I believe we should come to grips with the facts that they are a natural byproduct of the size and power of big government. As government has grown, and it has grown at a staggering rate, so too has governmental invasion of privacy.

One who knows well the insatiable appetite of the Federal bureaucracy for personal data is the former Director of the Office of Economic Opportunity, Howard Phillips. Mr. Phillips now directs a project known as Public Monitor at the American Conservative Union, and he has prepared the following brief commentary on the subject of government bureaucracy and the right to privacy.

[The information follows:]

BUREAUCRACY A THREAT TO PRIVACY

(By Howard Phillips)

Intrusions on the privacy of each citizen increase as the size and power of government increase. For every "benefit" we receive, there is a corresponding surrender of independence.

A bureaucracy which delivers social services is in a position to insist that the recipients of such services entrust to the agents of bureaucracy even the most personal information about their medical histories and family lives. Students whose education is underwritten with Federal dollars must respond to questionnaires which spell out their inner values and aspirations. Beneficiaries of government-backed credit must fully disclose the records of their financial history.

Further, when we rely on government, whether for food stamps or aspirin or legal services, how free can we be to challenge excessive intrusions? If the outreach worker helped us get a hospital bed when we needed it, might we not lose access to future help if we declined to acquiesce in a recommended sterilization procedure?

He who pays the piper calls the tune. Whatever government "gives" in services, it takes away from our opportunity to define the course of our private lives. The government which subsidizes defines the terms on which the subsidy may be provided.

Privacy increases as bureaucratic power declines.

Mr. DELLUMS. Mr. Speaker, I congratulate the gentlemen from California (Mr. Goldwater and Mr. Edwards), the gentlemen from New York (Mr. Horton and Mr. Koch) and the gentleman from Pennsylvania (Mr. Moorhead) for bringing this critical issue before the Congress.

For it is up to us here in the peoples' branch of Government to act quickly to protect the people of this Nation from the already too numerous encroachments upon their personal privacy.

It is frightening enough for a public official to realize that he is not only under constant public scrutiny, but that many aspects of our private lives are being watched—often illegally—day and night. But when I read of the lists and practices of various means of keeping tabs on millions of our constituents, then I am indeed alarmed about the future of the individual in this Nation which was founded and dedicated to individualism.

Too often we hear the claims that notions of privacy are inconsistent with the needs of a huge, technocratic, bureaucratized society. Yet it is only because we have allowed this Nation to become so huge, so technology-oriented, so bureaucratized that these assaults on privacy have increased.

And so, while I strongly endorse the need for positive legislative action to restore individual privacy, I also warn that this action cannot come within a vacuum—and that we must analyze also what caused the loss of privacy and what

ethical and institutional changes must also be accomplished before we realize this important goal.

Mr. O'BRIEN. Mr. Speaker, one of the most basic rights a citizen has, the right to personal privacy, has fallen to a deplorable state. As Senator Long so succinctly stated:

"Modern Americans are so exposed, peered at, inquired about and spied upon as to be increasingly without privacy, members of a naked society."

This speech was delivered to the Association of Federal Investigators on February 25, 1965, more than 9 years ago.

Since then, private insurance and credit agencies and such governmental agencies as the FBI, CIA, Secret Service, Department of Health, Education, and Welfare, and social security have gathered together scraps of information until today, there are dossiers on more than 100 million Americans.

The widespread use of computers with their vast capacity for compiling, storing, and swiftly retrieving these records compounds the problem.

One aspect of the privacy question that has attracted high level attention is the maintenance of criminal history records.

Each year an estimated 50 million Americans are arrested for some violation of the law. In 20 to 30 percent of these cases, charges are dropped immediately. In addition, 2 million of the 8.7 million arrested for nontraffic violations are not convicted.

The arrest information is diligently filed with one or several local, State, or Federal computer data banks. However, the record rarely shows the actual disposition of the case.

This sort of inaccuracy can cost a person his reputation, job opportunities or a legitimate credit rating. Even when a file is sealed or destroyed at one data bank, there is no guarantee that the information is not available at another bank. The reason is that data banks pass information from one to another similar to the Biblical woman who spread rumors like feathers in the wind.

The same problems apply to school records and financial histories that also follow a person through life. In many cases, individuals do not even know these records are kept. Even when they do, the subjects of the files have difficulty gaining access to the file and cannot challenge the accuracy of information it contains. Ironically, anyone labeling himself a "potential employer" or "potential landlord" has easy access and can study these records at length.

Such insidious invasions of personal privacy shake the very foundation of our constitutional right "to be informed of the nature and cause of the accusation and to be confronted with the witnesses against" us.

For these reasons, I introduced H.R. 11245 and cosponsored H.R. 9935, two pieces of legislation designed to correct at least some of the abuses of privacy.

The first of these, entitled the Fair Information Practices Act, would: forbid the maintenance of secret personal data systems; provide a means for an individual to find out what information about him is contained in a record and how it is used; allow the subject to prevent information about him collected for one purpose to be used for another without his consent; and give the subject a means for correcting or amending records containing identifiable information about him. Furthermore, any organization creating, maintaining, using or disseminating records of identifiable personal data would have to assure the reliability of the data for its intended use and would have to take precautions against misuses of the data.

The second bill forbids inspection of income tax returns by any Federal agency except under a Presidential order expressly identifying the person who filed the return.

As my colleagues may remember, the Secretary of Agriculture was granted permission last year to authorize any departmental employee to inspect a farmer's tax returns to determine the size of his farming operation. Fortunately, President Nixon recently rescinded that permission.

This bill would reduce the possibility of such wholesale examination of tax returns in the future for purposes other than collecting taxes.

These measures would safeguard citizens against snooping practices that reduce life to a fishbowl existence. Therefore I urge your support for this legislation.

Mr. BURGENER. Mr. Speaker, one of America's great champions of individual freedom and liberty is Senator Barry Goldwater, of Arizona. He is looked upon as a symbol of leadership and good judgment in Washington. Recently, he testified before the Senate Subcommittee on Constitutional Rights on his concern over the right to privacy in America. It is an eloquent statement. This message should

be read by all, especially by those of us in the Congress empowered by the people to legislate protections of human liberty.

Mr. Speaker, I am proud to include Senator Goldwater's statement with my remarks:

[The statement follows:]

WHO WILL PROGRAM THE PROGRAMMERS?

(Testimony by Senator BARRY GOLDWATER before the Senate Subcommittee on Constitutional Rights, March 6, 1974)

Mr. Chairman, it is a pleasure to join you today in your latest hearings on the subject of Computers and Privacy, a matter which I believe you investigated extensively in 1971. Though the primary focus of your current hearings is upon the use of criminal justice data banks, I know you are interested in the general subject of personal data bank systems and the ominous trend to national population numbering.

Mr. Chairman, I will devote my testimony to this broader subject because I have introduced legislation, S. 2810, which is now pending before this subcommittee, to establish safeguards for the individual regarding the keeping, use and accuracy of automated personal data systems of all types. The credit for having initiated the bill should honestly fall upon the shoulders of my son, Congressman Goldwater, Jr., who first introduced it in the House last September.

Mr. Chairman, we are not speaking about an alarmist's flight of fantasy. The computer era is already upon us. There are currently 150,000 computers in use in the United States, and some 350,000 remote data terminals. Conservative estimates indicate that there will be 250,000 computers and 800,000 terminals by 1975. Over 10% of all business expenditures on new plant and equipment in America is currently spent on the computer and its subsidiary systems.

Revolutionary changes in data storage have taken place or are imminent. Computer storage devices now exist which make it entirely practicable to record thousands of millions of characters of information, and to have the whole of this always avalable for insant retrieval. For example, the National Academy of Sciences reported in 1972 "that it is technologically possible today, especially with recent advances in mass storage memories, to build a computerized, on-line file containing the compacted equivalent of 20 pages of typed information about the personal history and selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds."

On larger systems today, the basic unit of time measurement is the nanosecond—one billionth of a second. It is hard for us to conceive but one nanosecond is to one second what one second is to 33 years!

Distance is no obstacle. Communications circuits, telephone lines, radio waves, even laser beams, can be used to carry information in bulk at speeds which can match the computer's own. Cross-country, trans-Atlantic, and inter-stellar transmission between computer units is now feasible.

Time sharing is normal. The time sharing systems with which we are familiar today are adequate for up to 200 users who are working at the same time. But we are now hearing of a system whereby it is feasible for there to be several thousands of simultaneous users of terminals.

An international body of experts who surveyed this subject in 1971 concluded that it is likely that, within the next 20 years, most of the recorded information in the world will be on computers and more than half the telephone calls will be communications to and from computers.

What does all this mean to you and me? How are we personally involved or associated with these developments? All we have to do is think of our daily lives.

Details of our health, our education, our employment, our taxes, our telephone calls, our insurance, our banking and financial transactions, pension contributions, our books borrowed, our airline and hotel reservations, our professional societies, our family relationships, all are being handled by computers right now.

As to strictly governmental records, it was calculated in 1967 that there were over 3.1 billion records on individual Americans stored in at least 1,755 different types of Federal agency files. Need I remind anyone that unless these computers, both government and private, are specifically programmed to erase unwanted history, these details from our past can at any time be reassembled to confront us?

Also, I might mention census data, which most of us think as being sacrosanct. Even census statistics, forbidden by law from disclosure in identifiable form, can be quite revealing.

The Census Bureau operates a popular line of business selling statistical summaries broken down into census tracts covering urban neighborhoods as small as a thousand families each. Any person or any organization can purchase this information which, while not containing specific names, does give a detailed outline of a small sector of the population, with size and type of housing, the way people travel to work, their type of work, their ages and sexes, all in a given neighborhood.

This information could be very valuable to those who would manipulate or influence social conduct. Matching other lists which already exist, relatively simple computing equipment can enable anyone wanting to know to determine the location of all persons in a small category. Thus, we can lose our anonymity without knowing it. Without our awareness, we become vulnerable to the possibility that this information can be put to use by administrative planners or policy makers for purposes of our social manipulation or conditioning.

If this were not enough, I might remind my colleagues that in 1966, the then Bureau of the Budget brought before Congress a comprehensive proposal to create a vast computerized national data center which would serve at least 20 different federal agencies. The people who proposed and evaluated this recommendation for the government, testified at House hearings on the matter that there was no way to avoid keeping records about specific individuals and individual attributes in this data center. Each of the government witnesses admitted that the records that would be included in the central data bank would leave a trail back to particular individuals.

Although this idea was put aside for the moment, after being exposed in the glare of Congressional scrutiny, the time to think about the future is now. We must design the safeguards, and set the standards, of personal privacy now while a national numbering system is still only a mental concept. We must program the programmers while there is still some personal liberty left.

The question we must face was posed by Malcolm Warner and Michael Stone, a behavioral scientists and a computer scientist, who ask in their book, The Data Bank Society:

"If one central source has all the data concerning our life history, and is bent upon regulating our behavior to conform to the prescribed goals of society, how can this be opposed? Only by the society demanding that sufficient thought be taken before the threat becomes a fait accompli.

What these writers recognize is that a welfare-statism society, in order to control its members, needs information. Total control requires total information. On the basis of this information, conclusions can be drawn, plans can be made, for directing us.

Other writers reach the same conclusion. Paul Muller and H. Kulhmann, writing in the International Social Science Journal, conclude that:

"Integrated information-back systems, at least looked at from the aspect of privacy, might bring with them the imminent danger of a one-sided alternation of the relationship between institutions and individuals, with the possibility of the individual's becoming open to scrutiny by the institutions, while the institutions themselves remained as complex and 'inscrutible' as before. . . .

Mr. Chairman, what we must alert to is that the computer society could come about almost by accident, as computers proliferate and integrate.

We did not start to build a nationwide telegraph network in the 1840's only independent telegraph links. But it was not long before we had an integrated national network.

We did not start to build a nationwide telephone system in the 1890's. Yet, today we have a highly integrated telephone network.

Automated information systems have the same qualities as communications systems. It is cheaper to share information by tying together independent systems than by building a great number of duplicative systems.

Thus, we are building today the bits and pieces of separate automated information systems in the private and government sectors that closely follow the pattern to the present integrated communication structure. The direction of growth is clear. Increasingly, data stored in computer memory banks is being shared by several users. Independent credit systems built to cover small areas find it economical to cross-connect. Airline systems swap information back and forth to get reservation information on individuals.

It is no wonder that in the summer of 1972, the International Commission of Jurists, in publishing a study on the right to privacy in ten Western nations, concluded that: "The latest and potentially the greatest threat to privacy is the recording, storing, and dissemination of personal information by computers.

Mr. Chairman, it is the theme of my testimony that, as we move closer and closer to a fully data-banked society, privacy must be planned beforehand. It is for us to determine today just how much freedom shall remain for the individual in the future.

Mr. Chairman, I would propose to answer this challenge by legislating into law a Federal code of safeguard requirements for automated personal data systems, the first law of its kind in America.

My proposal is generally consistent with the recommendations of the Secretary's Advisory Committee on Automated Personal Data Systems of the Department of HEW. This landmark report, canvassing the total impact on the individual, is a logical starting point from which Congress can begin to mold its own solutions.

The basic proposals of the Secretary's Committee, as I have incorporated them into S. 2810, are these:

1. There must be no personal data system whose very existence is secret.

2. There must be a way for an individual to find out that information about him is in a record and how that information is to be used.

3. There muse be a way for an individual to correct information about him, if it is erroneous.

4. There must be a record of every significant access to any personal data in the system, including the identity of all persons and organizations to whom access has been given.

5. There must be a way for an individual to prevent information about him collected for one purpose from being used for other purposes, without his consent.

The only exception which my bill would make from these general rules is where I believe it is necessary to protect broader national interest in the public safety, particularly in the categories of classified foreign affairs and defense secrets and criminal justice records which are pertinent to legitimate law enforcement purposes. If the exemptions of my bill are not broad enough, I am willing to make needed changes for the public safety. In this time of highly organized criminal forces who are mobile worldwide, I feel strongly that we should not tie the hands of those who would protect us in back of themselves.

Mr. Chairman, another important provision of my bill would stop the growing use of the social security number as a national population identifier. There already have been issued a total of 160,000,000 social security numbers to living Americans.

These numbers are used not only for the social security program, but for State unemployment insurance programs; for Federal and State taxpayer identification; for identification of all Civil Service employees; for registration of all purchasers of United States Savings Bonds and other government securities; to identify FAA pilot records; to identify all recipients of State old age assistance and medicare benefits; to identify the retirement records of all Civil Service retirees; for Veterans Administration hospital admission numbers; to locate the medical histories of many Indians; as the Service number of all military personnel; to identify all customers of banks, of savings and loan associations, of credit unions, and of brokers and dealers in securities; for use in receiving drivers licenses; to identify all applicants and beneficiaries of public assistance programs; to identify aliens working in the United States; and to identify children in the ninth grade and above in many school systems, among other uses not mentioned.

No statute or administrative rule prohibits use of the account number in other record systems. Indeed, an Executive Order by President Roosevelt is still in effect requiring that any Federal agency establishing a new system for personal identification must use the Social Security number.

Mr. Chairman, it is time to halt this drift towards reducing each person to a number. Professor Charles Reich has aptly referred to the idea of giving each person a population number as tying a tin can around him. All the rest of his life, he would have this tin can jangling along behind him. We would all become marked individuals.

A national population number would deprive us of what anonymity we each retain as individuals. Once identifiable to the administrator in government or business, by an exclusive number, we would become vulnerable—to being

located wherever we are, to being manipulated to being conditioned, to being coerced.

It is my belief, Mr. Chairman, that in order for the individual to truly exist, some reserve of privacy must be guaranteed to him. Privacy is vital for the flourishing of the individual personality.

By privacy, I mean the great common law tradition that a person has a right not to be defamed whether it be by a machine or a person. I mean the right "to be let alone"—from intrusions by Big Brother in all his guises. I mean the right to be protected against disclosure of information given by an individual in circumstances of confidence, and against disclosure of irrelevant embarrassing facts relating to one's own private life, both elements having been included in the authoritative definition of privacy agreed upon by the International Commission of Jurists at its world conference of May, 1967.

By privacy I also mean what the Supreme Court has referred to as the embodiment of "our respect for the inviolability of the human personality" and as a right which is "so rooted in the traditions and conscience of our people as to be ranked as fundamental."

Mr. Chairman, I call upon Congress to protect the right of privacy by enacting the safeguards I have proposed. In addition, I call upon the Executive Branch to take the following immediate steps.

First, the President should announce privacy requirements under section 111 of the Federal Property and Administrative Services Act of 1949, which allows him to establish "uniform Federal automatic data processing standards" for all computers used by Federal agencies. Second, a Citizen's Guide to Files should be issued by each government agency, specifying the nature of each of its files containing information about individuals; the class and number of persons covered; the uses to which the file is put; and whether individuals have access to any of their records in the file. Third, the President should cancel the Executive Order of 1943 which now spreads the use of the social security number.

What we must remember, Mr. Chairman, is that privacy in a data bank society must be planned. Privacy, as liberty, is all too easily lost. I urge that you act now while there is still privacy to cherish.

Mr. VEYSEY. Mr. Speaker, one of the fundamental rights granted by the fourth amendment to the Constitution is protection against unlawful search and seizure. In recent years, the courts have wisely extended this to include the individual's right to privacy.

Until the advent of computer technology, the spectrum of problems concerning the invasion of privacy was limited by geography. Now, however, there is a series of national data banks that can spit out the life history of almost any individual who has ever purchased a house or bought an automobile. The ease with which this information can be obtained by almost anyone for a small fee makes it imperative that standards be established to determine who has rightful access to such information and for what reasons it may be disseminated. This is a broad and complex problem today. There is a need to develop statistical data to interpret the socioeconomic trends that continually mold the culture of this Nation, but there is a fine distinction to be drawn between data collected for justifiable purposes and the secondary purposes for which the data is sometimes used.

The agencies that collect data relative to the extension of credit and the sale of life insurance perform a necessary service for the Nation's financial institutions. We must not severely restrict the legitimate services performed by these agencies; yet, we must develop adequate controls whereby information on an individuals personal affairs cannot be bought and sold indiscriminately.

In our efforts to control unwarranted invasions of individual privacy, we must take adequate precautions that we do not unduly handicap law enforcement activities. Data banks such as the one compiled by the National Crime Information Center have been criticized, but they provide an invaluable service to local law enforcement activities. A fugitive on the run can easily disappear, but in a matter of minutes, local police officials can check with the National Crime Information Center and turn a citation for a traffic offense in Florida into the apprehension of a murder or kidnaping suspect wanted in California.

The function of organizations that compile criminal statistics should be reviewed by the Congress, and if the need exists, minimum standards can be established as to the type of information that can be recorded, the length of time it can be held, and a convenient method for finding and correcting any errors that may occur.

The agencies that collect and maintain such information systems must be held responsible to see that their personnel comply with the statute. Civil damages awarded by court decision should be limited to compensatory rather than punitive damages, and adequate provisions must be included for criminal action against those who deliberately violate the statutes.

Mr. Speaker, this is a matter of prime importance, and I am pleased to see the interest that has developed in support of this legislation. I urge my colleagues to join with us in finding a reasonable solution to this problem.

Mrs. HOLT. Mr. Speaker, I would like to commend my colleagues for taking the initiative in focusing congressional attention on the important issue of personal privacy.

The rapid growth of Government and advanced communications technology has resulted in serious incursions into the domain of personal privacy. This issue knows neither philosophical nor partisan boundaries. The right to individuality is treasured by many institutions in America. Elected officials and national organizations which span the entire philosophical spectrum are united in their concern over the erosion of personal privacy and committed to safeguarding this democratic right.

Recently, the 185th general assembly of the United Presbyterian Church adopted "Guidelines for the Preservation of Privacy" along with recommendations for the implementation of these guidelines. They are positive steps which deserve serious consideration. I would like to include an excerpt of this document at this point:

[The information follows:]

GUIDELINES FOR THE PROTECTION OF PRIVACY

We call upon public and private agencies to provide for maximum protection of privacy in their dealings and transactions with each other and with individuals; and through self-regulation to meet at least these minimum guidelines for the collection, retention, and dissemination of personal data:

1. Determine beforehand whether the information to be gathered is necessary and relevant to the purpose for which it is sought, so as to minimize the amount of unduly personal, potentially injurious material that is collected and preserved.

2. Limit information systems to specific uses and justify the objectives, methods, and effects of any collection of personal data.

3. Give the subject prompt notice and ready access to such information. (We recognize that certain government agencies collect information on criminal activities where notice and access are controlled by established rules of law and procedure.)

4. Provide means for rapid correction of erroneous data, and the opportunity to expunge irrelevant or obsolete recorded data, such opportunity to be available to both the custodian and the subject of the data.

5. Provide effective safeguards to prevent accidental or unauthorized interception, input, or destruction of data.

6. Require effective safeguards for waiver of privacy and authorization of access to personal data executed by individuals and given to business, professional, and governmental bodies.

7. Limit the use and transfer of information in such systems, and monitor their expansion into enlarged data-sharing operations.

Mr. FAUNTROY. Mr. Speaker, I am extremely pleased to have the opportunity to join in this special order on privacy. The issue is one which we in this Congress must address with a vigor that will assure all Americans and the entire world that we mean what the words in our fourth amendment so clearly say.

Last year, it was my privilege to speak on this issue. While some of the facts are now a little dated, I am going to enter this statement as my contribution to this order, because I think that ome of the issues then raised have been forgotten. Some of the issues seem to have gone away, because political campaigns for the Presidency have gone away—at least for a little while—and we have a new FBI Director and a new Army composed of volunteers.

Perhaps some things have changed. But, I think it is good for us to refresh our memories on the horrors that have gone before in order that we do not allow ourselves to become complacent. If these transgressions have occurred once, they can occur again and again unless we take positive steps to end it.

The responsibility is ours—it is not the responsibility of anyone else. We use the people's representatives and it is time that we assure them that we have not

forgotten them and their right to be free Americans in a year when that question has been raised more vividly and clearly than at any other time in our Nation's history.

[The speech follows:]

PRIVACY AND POLITICAL SURVEILLANCE

(By Walter E. Fauntroy)

Privacy—that precious and most elemental of man's rights—defined by Justice Brandeis in an 1890 law review article as "the right to be let alone" is rapidly become more and more difficult to secure. I do not know how it has happened—perhaps, it has been the long years of war and international crisis that have created it. But we have become an "uptight society." The climate resembles the tempest set loose after the Korean War known as McCarthyism. Some in our society are afraid of "plotters" and subversives", and find them everywhere, even among those advocating peaceful social change.

In response to the admitted increase in wiretapping, eavesdropping, and other forms of surveillance, people have become increasingly afraid to communicate ideas or express opinions particularly if they be politically unpopular. Debugging of telephone lines, private homes and businesses has become a new industry. Some people accept the weekly visits from the electronics expert as a necessary fact of life. Even the House had had to retain the services of an independent electronics form to make periodic checks to discover hidden microphones in its facilities. As *Newsweek* observed in an article published last year and so aptly titled, "Is Privacy Dead?" "Somewhere in the roll of expanding population, vast economy, foliating technology and chronic world crisis, individual Americans have begun to surrender both the sense and reality of their own right to privacy . . .".

Justice Brandeis showed great wisdom in his dissenting opinion in the first wiretap case to reach the Supreme Court, *Olmstead* v. *United States*, decided in 1927, when he credited the Framers of the Constitution with having "conferred, as against the government, the right to be left alone—the most comprehensive of rights and the right most valued by civilized man." (277 U.S. 438, 478)

In view of the present revelations of governmental intelligence activities, Brandeis showed unusual foresight when he also wrote in his *Olmstead* dissent.

"Now subtler and more far reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government. By means for more effective than stretching upon the rack, to obtain disclosure in the court of what is whispered in the closest," (277 U.S. at 473)

Brandeis urged that to protect the right of privacy nothing less than prevention of "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

The difficult question for all of us, particularly federal, State and local law enforcement officers to decide is where intrusions upon our privacy are justifiable. On both the public and private levels, our complex economy requires some collection of data on each of us is necessary so that welfare plans can be designed to adequately service our needs and so the schools, hospitals, restaurants, department stores and airlines can extend immediate credit or otherwise serve the needs of the millions of people they must serve but have never seen before.

But, just because some intrusions on that essential part of our individuality are necessary and indeed inevitable does not mean that we should blindly accept all encroachments on our privacy. The nearly miraculous capacity of modern science and technology that have increased the powers of government and private industry to manipulate or interfere in the lives of individuals often stuns us into the belief that nothing can be done to reverse the destruction of our privacy. Surely one of our greater dangers is the perpetuation of this very attitude of hopelessness at a time when we are developing a technology that can manufacture miniature microphones or even adopt novel uses of laser beams to transmit sound and remove walls and distance as barriers to those who would attempt to seize our innermost secrets and search our thoughts.

While the subject of this discussion is invasion of privacy generally, it would seem to me that the issues raised by surveillance by federal officials highlights the dangers to our liberties. For us in the District of Columbia, distinguishing between local and federal activity is very difficult because local and federal are

intertwined. I will focus on federal activity today that invades the privacy of citizens largely because we, unfortunately, know so little about activity by local government. It has been shrouded in a veil of secrecy, without the national exposure that has recently been thrown on federal activity. I hope we can learn more soon so that remedial action by concerned local government and the Congress can begin on this front as well. The time cannot be too soon. But I think it's fair to say that the patterns of local and federal interference are similar and that in many situations local officials supplement and assist federal surveillance.

The area in which government investigation causes the most serious and threat to our constitutional rights is in the area of political surveillance conducted in the name of national security. The first revelations of our present domestic spy networks came through disclosures made by former Army Intelligence Officers, and later reinforced by testimony before hearings conducted by the Senate Constitutional Rights Sub-committee, of widespread use of military intelligence agents to spy on politicians or those who express views critical of administration foreign policy. The surveillance has not been limited to persons who could be considered radical. Senator Sam Ervin charged, after hearing testimony from a former Army agent assigned to political surveillance in Illinois, and confirmed by others, that Army surveillance agents have spied on Senator Adlai E. Stevenson, III, former Illinois Governor Otto Kerner and about eight hundred other civilians in Illinois alone. The military intelligence group which was the subject of the revelations—the 113th with jurisdiction over the Middle West, allegedly began their concentration on civilian surveillance as early as June, 1968, and continued at least until June, 1969, the date at which the informant, Agent John M. O'Brien, received his honorable discharge from the Army. The dossiers collected on State and local officials, political contributors, newspaper reporters, lawyers and church figures, including such diverse people as Governor George Wallace, Abner J. Mikva, and Bobby Seale, occupy over 120 feet of space at Region 1 Headquarters in Chicago. I might add that it has been reported that my name is among those contained in such dossiers.

Army, Navy and Air Force intelligence units also mingled on the floors of both the 1968 Democratic and Republican Conventions with unsuspecting delegates, allegedly without the knowledge of convention leaders and party officials to, according to the official explanation, assist the Secret Service in the protection of Presidential candidates. Away from the Convention floors themselves, agents also operated from store fronts and hotel rooms and toured the cities of Chicago and Miami in unmarked vans, intercepting telephone and radio messages and feeding all their gathered information to the Pentagon.

To assure ready availabiliy of these and other similar reports, the Army distributed them over a nationwide teletype service completed in 1967 that gives every major troop command in the United States daily and weekly reports on virtually all political protests occurring anywhere in the United States. The Army CONUS (Continental United States) Intelligence Program provided blanket surveillance of civilian political activity, according to the Washington Monthly with reports sent to the F.B.I. and the Justice Department's interdivisional intelligence unit, despite suits brought by the American Civil Liberties Union and Congressional and public protest. The reports are stored by the Justice Department which Senator Ervin has said, without contradiction, stores names and data on at least 13,000 citizens.

Sometimes the data gathered by the military agents approaches the level of absurdity. There is a story that has been widely circulated of an agent who had been following Mrs. Coretta King during one of her speaking tours that would be humorous were it not for the pervasive fear created in our society by these intelligence activities and the damage that these collected reports can do to a person's reputation. The agent had been making regular reports on Mrs. King's activities and telephoned his superior to report that she had referred repeatedly to her late husband's "dream". Back came the order, "Find out what that dream was . . ."!

The disclosure of F.B.I. files stolen from Media, Pennsylvania, gave us all a rude awakening into the reality of where the central focus of this most-effective intelligence gathering agency's activities may lie. I must agree with the statement of Representative Henry Reuss, who upon learning that a file had been kept on his daughter, said:

"The F.B.I. has an important responsibility to investigate crime. Its mission is not to compile dossiers on millions of Americans, Congressman's daughters or

not, who are accused of no wrongdoing. They should stick to their mission." (Washington Post, April 13, 1971, p. A3)

The records stolen from Media indicate that the F.B.I. believed that the function of monitoring of political activities is nearly as important as its main function—detection of crime and apprehension of criminals. An analysis by the so-called "Citizens Commission to Investigate the F.B.I." revealed that forty percent of the stolen documents involved investigations of a political nature. Of the documents on political activity, two involved surveillance of right-wing organizations, ten of immigrants, and over 200 involve leftists or liberal organizations. Of the sixty percent concerned with crime, twenty-five percent of the documents involved bank robberies; twenty percent involved murders, rape and interstate theft; seven percent involved draft resistance; seven percent involved A.W.O.L. cases; and one percent involved crime, mostly gambling (New York Times, May 13, 1971, p. 18).

The stolen records gave us a frightening glimpse into an intelligence gathering process which, if allowed to continue, will lead to ever increasing restraint on political expression. The documents suggest that the subjects of investigation include not only the well-known domestic terrorists, a form of self-protection we realize is to some extent necessary, but also obscure persons only marginally suspected of illegal activity. Included in the stolen documents were orders or discussion of orders from J. Edgar Hoover that all student groups "organized to project the demands of black students" be investigated, that an investigation be undertaken of a Boy Scout leader who wanted to take his troop to the Soviet Union for a month or longer be investigated to determine if any attempts had been made by Soviet Intelligence agencies to recruit them, and other subjects giving us a preview of the growing world of "1984" around us now.

Student militancy on college campuses was of particular concern to Mr. Hoover as is indicated by his following memorandum, dated November 4, 1970, which said in part:

"Increased campus disorders involving black students pose a definite threat to the nation's stability and security and indicate needs for increase in both quality and quantity of intelligence information on Black Student Unions and similar groups which are targets for influence and control by violence-prone Black Panther party and other extremists . . .

"We must target informants and sources to develop information regarding these groups on a continuing basis to fulfill our responsibilities and develop such coverage where none exists."

One of the documents is quite interesting in that it reveals that the increasing infiltration of black power and peace groups by F.B.I. informers was designed, directly as well as indirectly, to chill political expression. A newsletter from the Philadelphia Bureau Office instructs agents to increase their interviews with persons from the New Left because—

"It will enhance the paranoia endemic in these circles and will further serve to get the point across there is an F.B.I. agent behind every mailbox.

"In addition . . . some will be overcome with the overwhelming personalities of the contacting agents and volunteer to tell all—perhaps on a continuing basis." (New York Times, March 25, 1971, p. 33).

When we look at who the F.B.I. proposed to use or is using as informants, we get even more of an Orwellian chill. One document encouraged local police departments to actively recruit Boy Scouts as informers. The Boy Scout program known as "Operation Safe" (Scout Awareness for Emergency) was actively carried out, at least in Rochester, New York. Identification cards were given to each of the boys with police, F.B.I. and other emergency telephone numbers written on the back. They were asked to watch out for and report any unusual activity or lack of activity in neighbors' homes, plus many other things, including criminal and "suspicious acts—persons loitering . . . around schools, neighborhoods and parks."

F.B.I. documents indicate the Rochester operation has been successful in recruiting 20,000 "extra eyes and ears for the police department." How can we expect to maintain the slightest degree of personal privacy if thousands of naturally curious Boy Scouts are encouraged to use their eyes and ears for the F.B.I.?

Other documents indicate that care should be taken by persons who might be considered suspicious or dangerous by the F.B.I. to avoid quarrels with their spouses. Last January, the F.B.I. was told by an informer that it would be a good time to contact the wife of a Black Panther because she was "very angry" at her husband "now and may be receptive." Other relatives have been unwittingly used as informants by F.B.I. agents. The mother of a college co-ed from

Drexel Hill, Pennsylvania, was called by an agent who identified himself as "a friend passing through Philadelphia" and was thereby able to gain information on the girl's whereabouts and activities.

Wiretapping and electronic surveillance provide another area threatening individual privacy. While the F.B.I. had been tapping telephones for years before Congress passed Title III of the "Omnibus Crime Control and Safe Streets Act of 1968", that Act gave the first official sanction on both the federal and state levels to an odious practice by which the private conversations of hundreds of innocent parties could be intercepted and recorded without their knowledge to provide incriminating evidence against a comparative few.

The Supreme Court made wiretapping and eavesdropping more difficult when it gave its opinion in *Katz* v. *United States*, which overruled the famous *Olmstead* I. Olmstead had held that wiretapping violated the Fourth Amendment prohibition against unlawful searches and seizures only when there had been an actual physical trespass on the property of the petitioner. *Katz* ended this rather technical property-based concept of search and seizure, and the theory advanced in later decisions that there are constitutionally protected areas beyond which eavesdropping or wiretapping could be conducted without violating the Constitution. *Katz* had been convicted of illegally transmitting wagering information over the telephone in interstate commerce on the basis of recordings of his side of telephone conversations obtained from listening and recording devices attached to the outside of a public telephone booth. The Court of Appeals for the Ninth Circuit affirmed Katz' conviction because "there was no physical entrance into the area occupied by" Katz. Also, the public telephone booth could hardly be considered to be a "private" area. But the Supreme Court reversed the conviction because of its realization that—to quote the language of the Court's opinion:

"[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection.

"But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected." (389 U.S. at 351–352)

The Court found that the surveillance in that case might have been valid had it been authorized by a search warrant issued by a magistrate informed of the need for such investigation, specifically on the basis on which it was to proceed, and of the precise intrusion upon privacy it would entail. This magistrate, who would be more "neutral" than the law enforcement officer pursuing suspects, under the Court's opinion, should have been given power to oversee the search by requiring officers to report periodically on their progress, or provide other similar safeguards to assure that the authority provided by the warrant was not exceeded.

In Title III, Congress provided federal and state officers, whose states adopted similar statutes, a procedure for obtaining a search warrant for wiretapping or eavesdropping which Congress believed would meet Constitutional requirements set by the Supreme Court.

John Mitchell was not lax in his use of this new authority. In a speech to the Kentucky Bar Association, he revealed that from January, 1969 to March, 1971, 315 Federal court-authorized wiretaps including 51 extensions, were executed. The wiretap law has apparently provided smiilar incentives to the states. In 1969, the latest year in which complete figures are available, eight States—New York, New Jersey, Arizona, Colorado, Florida, Georgia, Maryland and Rhode Island—obtained 269 intercept authorizations of which 241 were actually installed. During 1969, law enforcement officers were granted ample time to develop evidence. The average length of time for the initial installation authorization was 26 days with an average of 22 days granted for extensions. However, the actual period of operation of these devices varied from three hours to 220 days. The total period of time in which wiretapping or eavesdropping devices were in operation in 1969 was 9,019 days and 3½ hours.

But the reported taps constitute only the tip of the surveillance iceberg. Title III contains several exceptions to the prerequisite that the petitioner obtain court approval prior to beginning a tap, the most dangerous one being the national security exception. Under the law, the President may authorize the Attorney General to engage in wiretapping or eavesdropping without court authorization or supervision whenever he considers it necessary to preserve the national security. The Justice Department has interpreted this law as permitting them to use electronic surveillance devices against so-called "domestic subversives" as well as foreign subversives.

The "domestic subversive" may be nothing more than a person dissenting from Administration foreign or domestic policies. When we look at the names of some of the people who have been the object of F.B.I. taps in recent years—the late Dr. Martin Luther King, Muhammed Ali, Bobby Baker, Sister Elizabeth McAlister, and some of the leading Las Vegas gamblers—we must conclude that the net spread to catch "internal subversives" may be very broad indeed. When we realize that the standard employed by the Justice Department to describe the occasions on which domestic national security wiretaps and bugs may be authorized—where there are "attempts of domestic organizations to use unlawful means to attack and subvert the existing structure of government"—we cannot help but be struck by the wide discretion and broad power this would authorize. Particularly in times of deep political division, of change, of high emotion and exaggerated rhetoric, this standard would deliver the privacy of many of us to the discretion of the Attorney General of the day who may or may not exercise it wisely.

Time does not permit discussion of all the methods by which "Big Brother" is building its dossiers on increasingly large numbers of us such as taking photographs of demonstrators or of college students assembled to hear controversial speakers such as Dr. Spock. The issues created by these governmental activities, however, are the same and are magnified when we consider their increased ability to store and recover almost instantaneously such fragment of personal data as may be stored on any of us. For example, J. Edgar Hoover once informed the Senate Constitutionl Rights Subcommittee that the National Crime Information Center has almost 2.5 million active records in its computerized files which are linked to 104 law enforcement and control terminals in fifty states and Canada. The arrest records of the hundreds of innocent bystanders picked up in the Mayday dragnet in the District of Columbia and subsequently released without trial are probably among the data now in those terminals.

Hoover assured the Committee in his statement that the system "has been so designed as to pose no threat to individual privacy." Since no specific detail was provided as to how individual privacy is to be protected by this system that was designed to provide "a more efficient and rapid means of handling and exchanging information," we apparently are expected to trust the F.B.I. Director to use his files wisely and well.

The Army and F.B.I. files are not the only dossiers maintained on political activists. Senator Ervin has revealed that the U.S. Passport Office keeps a secret "lookout file" of 243,135 persons who Director of the Passport Office, Frances Knight says are "of questionable citizenship." The Secret Service maintains files on "about 50,000 persons" who might attempt to harm or embarrass the President or other high government officials. The Internal Revenue Service tapes store details from tax returns of 75 million citizens which are available at cost to the states and the District of Columbia. Many other agencies maintain similar information, also.

William Rehnquist has told the Senate Constitutional Rights Committee that the Nixon Administration will oppose any legislation that would hamper its domestic intelligence-gathering activities. He said that the Administration "will vigorously oppose any legislation which, whether by opening the door to unnecessary and unmanageable judicial supervision . . . or otherwise, would effectively impair this extraordinarily important function of the federal government." He also argued that the gathering of intelligence information does not violate anyone's constitutional rights.

I am not advocating elimination of all criminal records or an end to surveillance of persons who in fact create a real threat to government. But why should the man who searches our thoughts and words be subject to any lesser control than the man who searches a room under authority of a court-issued search warrant? The intelligence gathering process has grown because our ability to more easily gather, store, and use volumes and types of evidence previously unattainable, and by the fact that many agencies are unable to distinguish between dissent and subversion. The attempts to choke off political discussion and dissent has created deep-rooted suspicions between generations, races and political groups, which have greater potential for destroying our country than the conspirators and subversives the administration tirelessly pursues. As Alan Barth recently wrote in expressing the apprehension created by disclosure of the stolen F.B.I. files and the extent of surveillance of domestic activity:

"The fear itself is a disease more dangerous than subversion." It paralyzes the interplay of political forces and ideas that makes the American system work."

We do not yet know enough to offer final solutions to this dilemma. Obviously greater judicial supervision and control of intelligence gathering, both on the federal and local level; should be a first step toward solution. We have always valued the imposition of the neutral magistrate between the law enforcement officer who has a personal stake in successfully solving a crime and the person he pursues, and this concept belongs in this most comprehensive form of search as well. Obviously, a wide ranging Congressional investigation is in order to plumb the depths of the intelligence network in our country. Court cases and stolen files have only given us a glimpse of the iceberg that threatens to limt any effective political dialogue in this Country, hinders First Amendment freedom of association, and, if not controlled may eventually sink this Ship of State.

Mr. PEPPER. Mr. Speaker, I am pleased to join in this special order to express my long standing concern over the invasions of privacy that have increasing encroached upon the freedom of the individual. I especially want to point up an aspect of this problem which may not be covered by another of my colleagues.

Our mammoth record-keeping and modern communications make even a charge of wrongdoing a threat to the individual throughout his life. While we must press our fight against criminal activity, as I have done as chairman of the House Crime Committee, we must always be conscious that our goal is not to stigmatize but to rehabilitate and restore to full citzenship those who may have been involved in some crime or wrongdoing. This is especially true of our young people, who account for an excptionally large amount of certain types of crime and who must be salvaged and diverted from such behavior if we are to avoid creating a permanent class of criminals, a large class of individuals who cannot resume normal patterns of life and livelihood and who are doomed to perpetrate crime after crime upon their aw-abiding neighbors.

I would like, therefore, to call to the attention of this body an excellent article written by Judge Charles E. Cashman, an outstanding Minnesota juvenile judge, on the problem of confidentiality in juvenile proceedings. The following is a condensed version of his article in the August 1973 issue of Juvenile Justice:

[The article follows:]

CONFIDENTIALITY OF JUVENILE COURT PROCEEDINGS: A REVIEW

(By Charles E. Cashman)

Fundamental to the philosophy of the juvenile law is the characterization of the nature of juvenile court proceedings as noncrimial. The laws of the various states establishing juvenile courts seek to assure the noncriminal aspect of juvenile proceedings by providing for the confidentiality of the juvenile court record. Minnesota defines the juvenile court record as including any and all police records pertaining to juveniles and thereby extends confidentiality to the entire record.

Most, if not all, adherents of the juvenile court philosophy probably agree that the provisions of the Minnesota code found in one form or another in other jurisdictons, constitute the cornerstone of the juvenile court itself. In fact, it seems fair to state that these provisons not only justify, but are indeed essential to the very existence of this unique court.

Notwithstanding the mandate of the United States Supreme Court in the case of *In re Gault*, 18 L.Ed2d 527, juveniles do not yet have all the rights which are historically attendant to crimnal proceedings involving adults. For example, at least at the time of this writing, there is no right to trial by jury, nor is there a right to bail. It is suggested that the promise of noncriminalty and confidentiality is in the nature of a contract by the state with the juvenile wherein certain rights ordinarily accorded to a citizen in our judical system are relinquished by a juvenile in return for the assurance of confidentiality and the protection from a stigmatic record.

The noncriminal nature of juvenile court proceedings has been given lip service by both state and federal courts throughout the United States. There is every indication, however, that in actual practice confidentiality of juvenile court proceedings is not adhered to much of the time. Justice Musmanno of the Pennsylvania Supreme Court, dissenting in the cast of *In re Holmes supra*, vividly describes the situation:

"The Majority is of the impression that the adjudication of delinquency of a minor is not a very serious matter because "No suggestion or taint of criminality attaches to any finding of delinquency by a juvenile court." This statement stamps

the judicial imprimatur on the declaration of Section 19 of The Juvenile Court Law that: "No order made by any juvenile court shall operate to impose any of the civil disabilities ordinarily imposed by the criminal laws of the Commonwealth, nor shall any child be deemed to be a criminal by reason of any such order or be deemed to have been convicted of crime." These words are put together so as to form beautiful language but unfortunately the charitable thought expressed therein does not square wtih the realities of life. To say that a gradaute of a reform school is not to be "deemed a crimnal" is very praiseworthy but this placid bromide commands no authority in the fiercely competitive fields of every-day modern life.

"A most disturbing fallacy abides in the notion that juvenile court record does its owner no harm. The grim truth is that a juvenile court record is a lengthening chain that its riveted possessor will drag after him through childhood, youthhood, adulthood and middle age. Even when the ill-starred child becomes an old man the record will be there to haunt, plague and torment him. It will be an ominous shadow following his tottering steps, it will stand by his bed at night and it will hover over him when he dozes fitfully in the dusk of his remaining day.

"It is equally a delusion to say that a juvenile court record does not handicap because it cannot be used against the minor in any court. In point of fact it will be a witness against him in the court of business and commerce; it will be a bar sinister to him in the court of society where the penalties inflicted for deviation from conventional codes can be as ruinous as those imposed in any criminal court; it will be a sword of Damocles hanging over his head in public life; it will be a weapon to hold him at bay as he seeks respectable and honorable employment. It is easy to say that the record will not be used in court but it already has been introduced in this case against Joseph Holmes in the imperishable dockets of several courts, it has been printed in the briefs which the world can read, and it will be published in the decisions of the Superior and Supreme Courts.

"It would not be kind to name the many figures in the world of sports, politics, entertainment and letters who have been embarrassed, harassed and encumbered because of a juvenile court record. And when I see how the intended guardian angel of the juvenile court sometimes nods at the time that the most important question of all—innocence or guilt—is being considered, I wonder whether some of these public figures may not have been unjustly tainted in their childhood."

There were many who felt that Justice Musmanno, with his flair for the dramatic, was prone to overstatement. He, and those who supported his position, were dismissed summarily as mere cynics. Unfortunately, or fortunately, depending upon one's point of view, Justice Musmanno's words proved to be prophetic as the language of the United States Supreme Court in the case of *In re Gault, supra* illustrates. In the *Gault* case, Justice Fortas in the majority opinion stated:

"Beyond this, it is frequently said that juveniles are protected by the process from disclosure of their deviational behavior. As the Supreme Court of Arizona phrased it in the present case, the summary procedures of juvenile courts are sometimes defended by a statement that it is the law's policy "to hide youthful errors from the full gaze of the public and bury them in the graveyard of the forgotten past." This claim of secrecy, however, is more rhetoric than reality. Disclosure of court records is discretionary with the judge in most jurisdictions. Statutory restrictions almost invariably apply only to the Court records, and even as to those the evidence is that many courts routinely furnish information to the FBI and the military, and on request to government agencies and even to private employers. Of more importance are police records. In most states the police keep a complete file of juvenile "police contacts" and have complete discretion as to disclosure of juvenile records. Police departments receive requests for information from the FBI and other law enforcement agencies, the Armed Forces, and social service agencies, and most of them generally comply. Private employers word their application form to produce information concerning juvenile arrests and court proceedings, and in some jurisdictions information concerning juvenile police contacts is furnished private employers as well as government agencies."

A further example of the disenchantment with this aspect of the juvenile court proceeding is contained in "Task Force Report: Juvenile Delinquency and Youth Crime" published by the President's Commission on Law Enforcement and Administration of Justice. In a chapter of the Task Force Report entitled "The Juvenile Court—Quest and Realties," the following statement is made on page 91:

". . . dour sociological critics urge that it (juvenile court) contributes to juvenile crime or inaugurates delinquent careers by imposition of the stigma of wardship . . .", and, again, on pages 92 and 93, the following is stated:

"Social scientists familiar with the juvenile court and its problems in the main agree that one of the great unwanted consequences of wardship, placement, or commitment to a correction institution is the imposition of stigma. Such stigma, represented in modern society by a 'record,' get translated into effective handicaps by heightened police surveillance, neighborhood isolation, lowest receptivity and tolerance by school officials, and rejections of youth by prospective employers. Large numbers of youth appearing in juvenile court have lower class status or that of disadvantaged minorities, whose limited commitments to education already puts them in difficulties in a society where education increasingly provides access to economic opportunity. Given this, the net effect of juvenile court wardship too often is to add to their handicaps or to multiply problems confronting them and their families.

"Lest these seem to animadversion or imprecise charges, consider the hard facts that social welfare agencies can be identified which as a matter of policy, without delving into the facts of the case, arbitrarily refuse to accept as clients youth who have been wards of the juvenile court. The reality of stigma due to wardship is also borne home by the firmed policy of the Armed Forces, which may make it the grounds for rejection, or most certainly the bar to officer candidacy. The paradoxical expression of stigma often colors the statements of probation and correctional officers, even judges, who at certain stages of a youth's progress through juvenile court and beyond, openly label him as a type destined for failure.

"Proposals, laws, and administrative action to preserve the anonymity of juvenile court proceedings through closed hearings, sealing case records, and expunging records are probably worthy moves, but it is vain to expect them to eliminate the stigma of wardship and contacts with the juvenile court. In smaller communities, as one judge observed. 'Everyone knows about juvenile court cases anyway.' In larger communities strongly organized police departments can be expected to resist rigorous controls over delinquency records detrimental to their efficiency, and will search for ways to circumvent them. Employers denied information from juvenile courts often get the desired facts from the police.

"Expunging records is not the simple operation it may seem. In California it requires initiative from the party concerned and usually the assistance of an attorney; the procedure necessitates a hearing, and it may be complicated or impossible if a person has been a juvenile ward in more than one county. Private and public organizations can and do protect themselves by including questions about a juvenile record on application forms for employment or for occupational licenses, indicating that perjured replies will be grounds for rejection. The applicant has the unpleasant 'damned if you do, damned if you don't' choice of lying or revealing damaging facts about himself. Finally, it is doubtful whether total anonymity of juvenile court hearings and records is in the public interest.

"While the successful management of stigma by individuals is not impossible, the necessary insights and social skills are not given to many people, least of all immature youth or those struggling with other status handicaps. A number of social psychologists, including the author, believe that social rejections provided by such stigma may reinforce a self-image held by the individual that he is no good or that he can't make it on the outside. They may feed a brooding sense of injustice which finds expression in further delinquency, or they may support, strengthen, and perpetuate ideological aspects of delinquent subcultures. In this sense the juvenile court may become a connecting or interventing link of a vicious circle in which delinquency causes delinquency."

The application of confidentiality even varies from county to county within a state despite the fact that the same law applies to each county in any given state. This failure to comply with the provision for confidentiality and noncriminality has had devastating and grossly unfair, as well as unjust, consequences to the future of young people who have had occasion to appear in a juvenile court. As the U.S. Supreme Court stated, "The evidence is that the juvenile courts, as well as the police, routinely furnish information to the FBI, the military, various governmental agencies and even to private employers." For example, applications for enlistment in the military insist upon full disclosure of all juvenile court appearances and dispositions under the threat of court martial and dishonorable discharge from the service for fraudulent enlistment. It is not unusual for employment applications and applications for a fidelity bond to similarly require disclosure of a juvenile court record.

It is submitted that the practices of the juvenile courts, and of law enforcement authorities in general, with respect to the matter of confidentiality and non-

criminality, represent a failure to live up to the promise of the juvenile court philosophy and in fact constitute an outright violation, not only of the spirit, but of the letter of the law itself. What is perhaps even more serious, these practices constitute a betrayal of the trust in the juvenile court process by those juveniles who, upon being petitioned into court, candidly and forthrightly tell all as well as by their parents who encourage them to do so. More than anything else, these practices have caused the proceedings in the juvenile court to be equated with a criminal proceeding—more than anything else, the practices demand the application of basic due process to juvenile proceedings in the same way as they are to a criminal proceeding and, more than anything else, have precipitated, indeed necessitated, the mandate directed to the juvenile court by the U.S. Supreme Court in the case of *In re Gault, supra.*

Students of the juvenile court system appear to be of two minds: (1) those who feel that rigid adherence to complete confidentiality as a basic concept of the juvenile court system, is both desirable and idealistically correct but that in actual practice it cannot be accomplished and, even if it could be accomplished, to do so would precipitate a torrent of reaction, both private and official, resulting in legislation which would eliminate what confidentiality now exists and possibly bring down the entire juvenile court system as well; and (2) those who feel that complete and rigid adherence to confidentiality is not desirable, does not make sense and is, in fact, not ideally or otherwise, a concept of the juvenile court system and, more importantly, that its application would release upon society unstable and dangerous persons or at least protect such persons from detection by an otherwise unsuspecting public.

To those who argue that confidentiality is desirable but not practical, it may be said that it is not up to the juvenile court to decide whether it is practical or not. It is simply a matter of the court and the law enforcement authorities complying wih the letter of the law where there are provisions similar to those existing in Minnesota. In those states not having laws specifically prescribing confidentiality, it is a matter of the court adhering to a fundamental concept of the juvenile court system. It should be fairly clear that, in the name of the best interest of the juvenile and his rehabilitation, the juvenile court system constitutes some abridgement of constitutional and other rights and protections usually thought to be available to every citizen of this country. This abridgement contemplates, if not requires some consideration in the way of a commitment not otherwise available to a person in court—it is suggested that confidentiality is such a commitment. If this commitment cannot be kept by the juvenile court itself, then, indeed, the court and the entire specialized system of juvenile justice ought to be abolished. So it is that the court should not decline to honor the commitment of the juvenile court system simply because of an anticipated reaction of the public acting in the person of its legislature. If the legislature wants the law changed, let it change the law but not the court fail to carry out the law for fear of what the legislature may or may not do.

With respect to those judges that feel confidentiality is not desirable and that to adhere to it would turn loose on the unsuspecting public the unstable, the dangerous, the psychotic and the psychopathic, an answer seems to be quite apparent. Most, if not all, juvenile courts have available some process whereby a juvenile offender may be referred to the prosecuting authority for handling as though the juvenile were an adult. In Minnesota this process is described as a reference for prosecution. The discretion to refer for prosecution is vested in the juvenile court. In some states, however, the discretion rests with the county attorney in choosing the forum for prosecution or litigation of the problem. In any event, this discretion is premised on the amenability of the juvenile involved to juvenile court processes or the public safety not being served under the provisions of laws relating to juvenile courts. Therefore, when the court proceeds with a matter, there is an implied finding that the person before the court is, in fact, a child markedly lacking in judgment, maturity and experience and, presumably is not, and should not be, accountable to the same degree as an adult.

If the court feels that it is dealing with a person who is so unstable or so dangerous that public safety would be jeopardized, presently or in the future, by a confidential record, then, most assuredly, such a court may refer the matter for prosecution as an adult. Two things would thereby be accomplished, (1) the hearing and the record would be made public and, (2) the young person charged would have the full protection of all constitutional, statutory and case law guarantees available in the state's criminal law process. All of the rights of the in-

dividual historically sacred in this country as expounded in *Miranda, Escobedo, Gideon, Mapp* and other landmark cases in the U.S. Supreme Court and the various state supreme courts, would then be available to juveniles just as they are now to any other U.S. citizen.

In other words, the juvenile court's discretion to waive or retain jurisdiction seems to place a responsibility on the juvenile court to make some determination as to the kind of person it is dealing with in any given case. Wherein it determines that one is a juvenile then that person should be accorded the protection a child should have. On the other hand, if the court determines that a person, though a juvenile by age, is accountable as an adult, then that person should be accorded all the rights of an adult, not just part of them. To hold otherwise is to unjustly expose thousands upon thousands of essentially normal and innocent young people to the damaging consequences of a juvenile court record.

It is said that the juvenile court system is rehabilitative in nature. It cannot be rehabilitative if the mere appearance in a juvenile court creates a record which will affiict a person for life and may thwart worthwhile careers and ambitions. It is a delusion to argue otherwise. If juvenile court proceedings cannot be kept confidential then it should be recommended that the entire juvenile court system be abolished and that the state should seek enforcement of its criminal laws in the regular processes of criminal court proceedings wherein the accused has the full protection and benefit of constitutional, statutory case law.

Mr. HARRINGTON. Mr. Speaker, I welcome the opportunity to participate in this special order on privacy, organized by my colleagues. Congressmen Kich, Goldwater, Horton, Moorhead, Kemp, and Edwards of California. It is heartening that so many Members of the House should join together to address such an important issue.

There has even been some encouragement from the White House in the area of privacy. President Nixon has at least recognized that Government encroachment into the rights and freedoms of individuals is a serious and growing problem, although his solution—yet another advisory commission—leaves something to be desired. Still, I hope that today's bipartisan display of support for protection of privacy is indicative of improving prospects of enactment of legislation strengthening the individual rights of citizens.

Basic rights and freedom are being violated daily by the computerized data banks now assembled on millions of American citizens. Criminal arrest records are virtually unregulated today. In thousands of cases, citizens are harmed by information on these arrest files which is inaccurate or incomplete. Most serious is the failure to require an indication on arrest records of the disposition of a criminal charge.

Mr. Speaker, almost a year ago, a particularly perceptive article on the subject of criminal arrest records appeared in the Sunday New York Times. I commend this article. "Have You Ever Been Arrested," by Aryeh Neier, to the attention of my fellow colleagues:

[The article follows:]

HAVE YOU EVER BEEN ARRESTED

(By Aryeh Neier)

On Jan. 18, 1970, Paul Cowan was arrested in Brooklyn for possession of marijuana. Two months later the charge was dismissed. In September, 1970, Cowan moved to Boston. He applied for a license to drive a cab. On Feb. 15, 1971, a hack license was issued, but a week later, on February 22, he was ordered to report to the Boston Police Department's Bureau of General Services and informed that his license was being revoked. The reason: a routine check with the Federal Bureau of Investigation had disclosed that an "open" charge of possession of narcotics was pending against Cowan in New York. He protested that the charge had been dismissed. No good. On March 12, 1971, Paul Cowan received formal notice that his license had been revoked because he was "not a suitable person to be so licensed." Cowan's story is unusual in only one respect. He found out why he lost his job. Most people who are denied jobs because of arrest records are never told the reasons.

In 1967, the President's Commission on Law Enforcement issued a series of comprehensive reports on crime in America that are still considered the definitive findings on the subject. The commission found that 58 per cent of white

urban males, like Paul Cowan, will be arrested at some time during their lives. (The figure for nonwhite urban males is 90 percent, for U.S. males in all categories 50 per cent; for all females it is 12 per cent.) Like Paul Cowan, many of those arrested are not convicted. In fact, of about 8.6 million persons arrested in 1971 for all criminal acts other than traffic offenses, nearly 4 million were not convicted. They are presumed innocent. In practice, they often suffer consequences as grave as if they had been guilty.

The F.B.I. is the major source of arrest-record information. As a matter of routine, almost all police departments in the country forward to the bureau for filing the fingerprints of persons they have arrested. (All persons fingerprinted upon induction into the armed services are also on record in the F.B.I. fingerprint files.) Testifying in the case of *Menard* v. *Mitchell* in 1970, a bureau official reported that, on the average working day, the bureau received 29,000 sets of fingerprints. Only 13,000 came from law enforcement agencies. The remaining 16,000 sets were sent in by banks, insurance companies, government employers (municipal, county, state, and Federal), licensing agencies and the like. In return, these agencies received from the F.B.I. whatever information it had in its files on the 29,000 persons involved. That's how Paul Cowan's Brooklyn arrest record got to the people who give out hack licenses in Boston.

While the bureau has been very efficient about gathering and disseminating arrest records, it has been fairly careless about including data on the disposition of the cases. In the Menard case, the special agent in charge of the F.B.I. Indentification Division, Beverly Ponder, got a little testy when questioned about this by a volunteer lawyer for the National Capital Area Civil Liberties Union, Raymond Twohig:

TWOHIG. Does the F.B.I. make any effort to obtain final dispositions where requests are received for arrest records? Before disseminating those arrest records?

PONDER. We urge the contributors [to the F.B.I. fingerprint files] to submit to us final dispositions, but we don't go out and try to pick them up.

Under further questioning, Ponder testified that there is no statistic available within the F.B.I. on the final dispositions that have been recorded in the bureau's files and that he knew of no way to make an intelligent estimate of them. That helps to explain how it happened that the Boston hack-licensing people weren't told that the charges against Paul Cowan had been dismissed.

Some employers are not interested in arrests, only convictions. One such, it was thought, is the Federal Civil Service Commission. Mr. Ponder was asked about that by Twohig :

TWOHIG. Is the F.B.I. aware that recently Federal job-application forms were changed, and the question which asked if the applicant was arrested now asks if he has been convicted?

PONDER. Yes. I am aware of that.

TWOHIG. Do Federal agencies, in particular civil-service commissions, receive at present all information about arrests—or only arrests with convictions—when they apply to the F.B.I.?

PONDER. They receive all the material that appears on the identification records.

TWOHIG. And that includes conviction and non-conviction arrests?

PONDER. That is correct.

The circumstances of this case were that Dale Menard, a former Marine, had been arrested by the Los Angeles police for "suspicion of burglary." He was never convicted or even prosecuted. In fact, it is not clear that a crime was committed by anyone. Menard had the misfortune to be sitting on a park bench in a neighborhood where the police had received a telephone complaint about a prowler. With the help of the National Capital A.C.L.U., Menard sued to remove his arrest record from the files of the F.B.I. and to stop the F.B.I. from reporting his record to potential employers. Menard's suit has been in court for more than five years. It has been heard twice by Federal District Courts and twice by the United States Court of Appeals in the District of Columbia, where it is now awaiting decision.

Back in June, 1971, the Menard case was the subject of a controversial decision by Federal District Judge Gerhard Gesell. He ordered the F.B.I. to stop distributing arrest records to anyone but law-enforcement agencies and then only for law-enforcement purposes. Gesell found "that Congress never intended to or did in fact authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks." He concluded that the arrest-record distribution system "is out of effective control."

Congress acted quickly to overturn the order. A bill introduced by Senators Alan Bible and Howard Cannon of Nevada was passed which made F.B.I. arrest data available to "any non-law-enforcement official or agency" authorized to get the information by state or local law. The two Senators said they were particularly concerned that the information be available to Nevada's gaming industry so that people with arrest records would be kept out.

The case for the bureau's role of maintaining and disseminating arrest records was recently set forth by L. Patrick Gray 3d, acting director of the F.B.I., in a written response to a question from Maryland's Senator Charles Mathias Jr., of the Senate Judiciary Committee, which was considering Gray's nomination as permanent director of the F.B.I. Gray wrote:

"The arrest-record files of the F.B.I. Identification Division as well as those of many state and local identification bureaus are replete with lengthy arrest records of longtime hoodlums and members of organized crime whose arrests never resulted in conviction. Many sex offenders of children are not prosecuted because parents of the victim do not want to subject the child to the traumatic experience of testifying. Others are not tried because key evidence has been suppressed or witnesses are, or have been, made unavailable. The latter situation is not uncommon in organized-crime cases. To prohibit dissemination of such arrest records would be a disservice to the public upon whom they [persons with records] might prey again."

Gray went on to speculate about "the potential school teacher with two prior rape arrests and no convictions" and "a police applicant with a prior Peeping Tom arrest and no conviction." Given these possibilities, "the rationale for disseminating arrest records not supported by convictions is substantial," said Gray.

Protesting this viewpoint, Ralph Temple, the lawyer who recently argued Dale Menard's current appeal, has commented: "That turns the Constitution upside down—it presumes guilt." Temple, who is legal director of the National Capital A.C.L.U., is trying to persuade the U.S. Court of Appeals in the District of Columbia that punishment by record dissemination, without trial and conviction, violates the Constitutional guarantee of due process of law.

Opposition to the dissemination of arrest records is mounting elsewhere. Representative Don Edwards of California and Senators Quentin Burdick of North Dakota and Sam Ervin Jr. of North Carolina are leading a fight to pass legislation prohibiting the F.B.I. from disseminating arrest records that do not result in convictions. Two United States Courts of Appeals have also recently found that questions about arrest records are racially discriminatory. Citing these court decisions, the New York City Commission on Human Rights issued "guidelines" on Jan. 4, 1973, stating that "it will be considered an unlawful discriminatory practice for employers or employment agencies to ask of any applicant or employee any questions relating to arrest records" or to solicit the information from another source. Illinois has passed a law making it an unfair labor practice to deny a job because of an arrest record.

The guidelines of the City Commission on Human Rights were an outgrowth of several days of hearings last year on employment difficulties faced by people with arrest records and people with conviction records. Those hearings were, in part, a result of the commission's earlier hearings on the employment practices of the Board of Examiners of the New York City Board of Education, which licenses teachers for the New York City public schools. The hearings had produced testimony about such things as the denial of teacher licenses to people arrested in civil-rights demonstrations in Mississippi. Another Board of Examiners case involved a young man, David Mills (not his real name), who had been convicted of a misdemeanor in New York City Criminal Court in December, 1969. In February, 1970, Mills applied for a license as a substitute teacher in the public schools. In May, 1970, he was summoned before the Board of Examiners to explain the circumstances of his conviction. At the time, Mills' conviction was on appeal, and he was assured by two examining officers that if it was reversed, he would have no difficulty getting a license.

In October, 1970, the Appellate Court unanimously reversed Mills' conviction "on the law and the facts." Mills immediately took a copy of the decision to the Board of Examiners. He then started to get a runaround. Even though he had taken the license examination the previous February, he was told for the first time that he now needed a "nomination" from a specific high school that wished to employ him. Next, he was told that his application had to be approved by the Board of Education's Department of Personnel. In late November, the Department of Personnel approved the license but the Board of Examiners still re-

fused to issue it, claiming more time was needed to investigate Mills' "criminal" record. Finally, with delay piled upon delay, Mills filed suit against the Board of Examiners to compel it to issue the license. In the face of the lawsuit, the Board of Examiners finally granted Mills his license in March, 1971.

The first court case to be decided on the basis that inquiries about arrest records are racially discriminatory was *Gregory* v. *Litton Systems*, a case brought by the American Civil Liberties Union of Southern California. At first glance, Earl Gregory, a Los Angeles black, seems an unlikely candidate for a test case. He had a record of no fewer than 14 arrests. Gregory had sought a job as a sheetmetal mechanic. Although he was otherwise qualified, he was turned down because "Litton's standard policy," it was stipulated in court, "is not to hire applicants who have been arrested on a number of occasions beyond minor traffic offenses."

Gregorys trial indicated that his arrest was not unusual. Dr. Ronald Christensen, one of the authors of the Report of the President's Law Enforcement Commission, who appeared as a witness, testified, that a person who has been arrested once tends to accumulate additional arrests during his lifetime, the average for a white man being 7; for a black man the lifetime average is 12.5 Christensen and another prominent analyst of crime statistics, Dr. Marvin Wolfgang, also testified that on one large category of arrests—on "suspicion" or for "investigation"—blacks were arrested about four times as often as whites. As an indication of how much importance could be attached to these arrests, Dr. Wolfgang cited a study of "investigation" arrests in 1964 in Baltimore, which revealed that 98 per cent of the persons arrested were released without further proceedings. The court also heard extensive testimony about studies which showed that persons who had been arrested on a number of occasions performed as efficiently and honestly on the job as persons who had never been arrested.

Litton Systems argued that the "business justification for considering a person's arrest record in determining whether or not to hire him is the same as considering a record of conviction. . . . It is not a fact, and it cannot be assumed, that all arrests which did not result in conviction are unfounded." The testimony by Christensen and Wolfgang proved to Litton "that people with arrest records are arrest-prone, and that the proneness increases with the number of prior arrests. There is business justification in declining to hire people with arrest records because the employer has a legitimate reason in not wanting to hire people who are more likely to be absent when they are arrested. . . ." While Litton cited no other "business justifications," the firm expressed a certain pique that it was being singled out for attack. An inquiry about arrest records, Litton told the court, "is one of the most common employment practices known to man. Almost anyone who has ever applied for a job has answered this type of question . . . the employer who does not obtain and utilize arrest information in determining whether or not to hire is the exception, not the rule."

Litton's arguments about the frequency with which employers rely on arrest records are supported by a February, 1972, report issued by the Georgetown University Law Center. The report was prepared under a grant from the U.S. Department of Labor. It found, that "the existence of arrest records is all-pervasive in our society and that millions of individuals may be hampered in the efforts at finding jobs and pursuing careers because of such records." Most state and county governments inquire about such records on job-application forms, according to the Georgetown report. Sometimes arrest records are absolute barriers to public employment, the report says, but more commonly they restrict applicants to low-skill jobs.

In its first decision in the Dale Menard case, the U.S. Court of Appeals in the District of Columbia cited a study showing that 75 per cent of the employment agencies in the New York area will not accept for referral applicants with arrest records. Another survey cited by the court showed that, of 75 employers, 66 would not consider hiring a man who had been arrested for assault although he had been acquitted.

The fact that Litton's policies were no worse than those of other employers did not deter a Federal court from awarding Earl Gregory $4,400 in damages because of the inquiry about his arrest record. In February, 1973, that judgment was upheld by the U.S. Court of Appeals in California.

The most sweeping action against arrest records was a recent decision by the Supreme Court of Colorado. The court ruled that arrest records of persons not convicted must be expunged unless the police can demonstrate the need to retain a particular record.

Dorothy Davidson, executive director of the Colorado A.C.L.U., was the plaintiff in the suit. She had been arrested in 1968 while trying to act as an observer at a police-hippie confrontation in Denver. (These arrests are an occupational hazard for local A.C.L.U. directors. In 1968, there were similar arrests in four other states. I was the director of the New York C.L.U. at the time and was arrested observing an antiwar demonstration in Manhattan's Washington Square Park. None of us were convicted.) The court found expungement of arrest records necessary because "the record here is devoid of any facts showing . . . the ability of the [Denver police] department to keep them confidential."

Only expungement can keep arrest records confidential, as has been demonstrated in New York. In 1964, the New York State Identification and Intelligence System was established. It was not supposed to be available for private-employment checks. However, in 1969, the State Legislature passed a law requiring the fingerprinting of all employes in the securities industry, one of the state's largest. Prints are now checked against the six million on file with N.Y.S.I.I.S. and the information is given to the State Attorney General, who makes it available to the employers. In his first report on the program, Attorney General Louis Lefkowitz announced with great pride that several hundred employes had been found to have "criminal records" and that many were fired. About half of those fired had no record of convictions, only arrests. A Federal District Court dismissed the New York Civil Liberities Union challenge to the fingerprinting and the decision was upheld on appeal.

Fingerprinting of employes had been sought by the securities industry as a means of trying to stop thefts. Fear of crime is always the reason for compiling and disseminating arrest records. The records presumably tell us whom we should fear and thus enable us to shield ourselves from them. The trouble is that people with records don't simply disappear from the face of the earth. They continue to live in our cities, many of them in our black ghettos. Having used their records to keep them out of our places of employment, we still have to live with them. Are they less likely to commit crimes because we can keep them from getting jobs?

Job problems are not the only consequences of arrest records. Consider the case of Mildred Brown. She has lived in a housing project on Manhattan's East Side for 20 years. The New York City Housing Authority recently found that she was "ineligible for continued occupancy on the ground of nondesirability," a finding based in large part on her son's arrest record. While no comprehensive studies have been done on housing problems growing out of records of arrests not followed by convictions, Mrs. Brown's case is not unusual.

Arrest records also affect chances for admission to educational institutions, opportunities for financial credit, and, as Litton's arguments about "arrest-prone" people suggest they increase the likelihood of re-arrest. A young black man in Washington, D.C., recently filed suit to stop police harassment growing out of his arrest record. He had been arrested while a senior in high school in May, 1970. In January, 1971, he was acquitted of a robbery charge because of an apparent case of mistaken identity. He is now a college student and a National Merit Scholarship winner. According to his court complaint, on at least three occasions police have shown his photograph in neighborhoods where crimes have been committed, seeking to have him identified as the criminal in some new crime. Each time this has been done, his family and acquaintances have been interrogated anew.

People with arrest records are natural targets for investigation when new crimes are committed. Inevitably, arrests follow. Being "arrest-prone," therefore, is often a function of having been arrested. The practice is to "round up the usual suspects," as police Capt. Louis Renault (played by Claude Rains) put it in the film "Casablanca."

Each year, law-enforcement agencies grow more efficient in disseminating records. The bureau's Identification Division, which was receiving 29,000 sets of fingerprints daily in 1970, is only a manual system operating through the U.S. mail. Recently, to supplement this service, the bureau established a computerized system, the National Crime Information Center, to speed the exchange of records with local law-enforcement agencies around the country.

Private industry is in the record-keeping and record-selling business in a big way. The biggest firm in the business, Retail Credit Company of Atlanta, has more than 7,000 employees, maintains dossiers on about 45 million people and produces more than 35 million reports a year. The members firms of a trade association known as the Associated Credit Bureaus, which among them do a business

of close to $1-billion a year, maintain files on about 10 million Americans. The information in these files is sold to creditors, employers and landlords.

Much of the information sold by the credit bureaus comes from law-enforcement files. There is no indication that the F.B.I. gives any information directly to a credit bureau. However, the F.B.I. has been notoriously loose in policing the further distribution of the records it disseminates. Here is the testimony on this point of Special Agent Ponder at the Menard trial:

Q. Is there any procedure whereby the F.B.I. or any division of the F.B.I. inquiries into the uses to which the arrest information is put by contributing agencies?

A. No.

Q. Are any restrictions imposed by the F.B.I. on the use to which that information is put?

A. Yes. Official business only.

Q. Are there memoranda or orders indicating that there is a restriction?

A. It is right on the record itself.

Q. Are there any form letters that are sent to contributing agencies explaining what "official business only" means?

A. Well, in years gone by we have brought this to the attention of contributors, that this information is disseminated strictly for official use only.

The questioning of Ponder took place on Dec. 17, 1970. Subsequently, he supplied for the court record the F.B.I.'s most recent notice on the issue, a memorandum from the late J. Edgar Hoover dated Oct. 18, 1965. If the records were used for other than "official uses," Hoover warned, "this service is subject to cancellation." No other penalty was mentioned.

The laws of many states provide that juvenile records are confidential. However, they have been as readily available as all other records. The F.B.I., which respects all state and local laws which confer access to records on various agencies, disregards state laws governing confidentiality. Special Agent Ponder was asked in the Menard trial, "Are there any differences in dissemination practices with respect to juveniles and adults, of arrest records?" His complete reply was: "No."

The New York State Identification and Intelligence System also gives out juvenile arrest records. When I asked the director of the agency about this, he told me that N.Y.S.I.I.S. understood the law to make the disposition of a juvenile-arrest confidential, but not the underlying arrest.

The widespread availability of law-enforcement records has created a pariah class of millions of persons made up of ex-convicts and people arrested but not convicted. That pariah class is the crime problem, or at least a large part of it. Crime is centered in those cities and those parts of cities where people go when they are trying to escape their past records. The time-honored way of escaping was to lie when asked, "Have you ever been arrested?" As law-enforcement agencies and private companies improve the efficiency of their dissemination of records, lying no longer works. The truth about the past record catches up, no matter where a person moves.

Shocking as the notion might be, those lies served an important social purpose. When a man with an arrest record could lie his way into a job all of us had a little less to fear. Today, when we expose the lie, we simply insure that one more person won't be able to escape his arrest record and integrate himself into society.

Judicial and legislative action to control the use and distribution of arrest records will not have much impact for a long time to come. The records of people arrested in the past have often been so widely circulated as to make it very difficult, if not impossible, to prevent them from continuing to haunt people for years to come. But action has to start sometime, and the best time is now. There is even a small sign that the F.B.I. is concerned. At the hearing last Feb. 28 to decide whether he should be confirmed as F.B.I. director, L. Patrick Gray testified that he had "purged inactive arrest records of individuals age 80 and older from the fingerprint files." All the octogenarians I know who are out looking for jobs are very grateful.

Mr. BUCHANAN. Mr. Speaker, we are today 10 years away from the 1984 of George Orwell, but to many of us, the Big Brother of which he wrote is with us already.

It is unfortunate that as the Federal Government has expanded to meet the needs of the American public, the rights of that same public to conduct its affairs in private has been sublimated to expediency, but this is not the way it was originally intended.

The framers of the Constitution spoke to this right in adopting the fourth amendment to protect the right of the people "to be secure in their persons, houses, papers, and effect."

But today, there is hardly a citizen anywhere in this land of more than 205 million people who is not recorded one way or another within the Federal bureaucracy.

The armed services, the Social Security Administration, the Veterans' Administration, the Internal Revenue Service, the Justice Department, the Census Bureau and the Bureau of Labor Statistics, to name but a few, have dossiers on many millions of Americans. The accuracy of this vast amount of information is, at best, questionable and, in most instances, the individual has no access to the files compiled on him and no opportunity to correct any misinformaiton.

The information, true or false, is shared with other agencies and, in some instances, nongovernmental agencies. Too often there has been the public release of raw information, in the form of rumors, gathered by one agency or another.

But it is not only the Federal establishment which is at fault. Private companies and organizations are often even greater offenders. An individual applying for a credit card from one company is often subjected to a flood of advertisements and solicitations from other organizations who purchased the mailing list of the original firm. In some instances not only the name and address of the individual involved, but other personal information is disclosed.

We have taken some action to protect the individual, such as the enactment of the Fair Credit Reporting Act of 1970, but it would appear that additional steps are necessary and many measures have been proposed.

I am concerned, however, that Members of Congress may not take these invasions of privacy quite as seriously as the average American because our lives are so exposed to public scrutiny. It is my hope that we will not become inured to the ever encroaching invasions on the privacy of our constituents. To the average American citizen, the right to privacy is a very real right which needs to be strengthened.

Mr. Speaker, I am happy to join with my colleagues in a commitment to privacy and urge that this verbal commitment be transcribed into actions which will restore to fact the right to privacy which exists too often only on paper.

Mrs. HECKLER of Massachusetts. Mr. Speaker, today's special order provides a welcome opportunity for this body to express its strong commitment to every American's inherent right—the right to privacy. I trust today's discussions will not only be a forum for enlightened discussion, but will also be legislatively productive.

Solitude for one's self and one's thoughts is essential in a free society. And yet, intrusions of privacy grab the headlines each day. The invasions are myriad—unauthorized drug searches, illegal wiretapping, false credit records, unrequested distribution of legal, mood-changing drugs, psychosurgery, and extensive student records concealed from the child's parents. It is these very abuses of authority which prompted me to introduce legislation which would create a Select Committee on Privacy.

Loss of privacy often occurs without fanfare and unbeknownst to the citizens affected. It is for this reason that the Congress desperately needs an ongoing watchdog committee which would discuss current and potential invasions of privacy while at the same time recommending corrective legislation. The Congressional committee structure as it now stands encourages a shotgun approach to congressional inquiry. No one committee has been delegated the responsibility for continuous study of the broad privacy issue and different facets thereof. Upholding the privacy of American citizens through the best congressional means available is far too important to delay 1 day longer.

The Select Committee on Privacy would have authority in numerous areas. Behavior modification in grammar school children would certainly be a priority issue. Thousands of elementary school students are administered amphetamines or Ritalin to alter their behavior because they have been labelled restless, inattentive, or uncomfortable with discipline. What schoolchild is not restless and inattentive at times.

Another area of overriding importance is the massive files collected by banks, credit unions, or the Federal Government. Though these files are reportedly "secure," numerous examples exist of selling collected data, access to sensitive material by unauthorized persons, merging of scattered files into complete "dossiers," and so forth. The real tragedy of these incidents lies in the often inaccurate information contained therein of which the person being studied has no knowledge. Disaster to livelihood, home, family and belongings have been known to occur as the result of gross misinformation.

One of the most frightening invasions of privacy has come to light only within the past few years. Psychosurgery and lobotomy operations which irreversibly mutilate healthy brain tissue in order to deal with psychological problems are most controversial. The potential unrestricted use of such operations to control patients exhibiting aggressive tendencies is alarming indeed.

These are only a very few of the numerous examples of privacy abuses. However, the mere existence of such illustrations magnifies the crying need for formal congressional oversight. The Select Committee on Privacy which I have proposed and continue to support would be a viable tool in guaranteeing the right to privacy of all Americans while at the same time controlling the innumerable abuses existing today.

Mrs. BURKE of California. Mr. Speaker, today's communications technology makes it possible to store virtually limitless amounts of information, and disseminate that information with almost unimaginable speed, from one point to another. This technology is being used to lay the groundwork for a vast national communications network, a potentially awesome weapon in this Nation's fight against crime. The application of this technology to other areas of investigation has undoubtedly facilitated the detection of persons engaged in "suspicious activities," of persons who might be "bad credit risks," and indeed of persons of every conceivable character and any given description: the only technical limit to this system is the extent of the information on file.

While making the greatest possible use of these resources, however, we must keep in mind the U.S. Constitution, which provides that the people have the right to be secure in their persons and property from "unreasonable searches and seizure," the right to receive and impart information and ideas without fear of harassment and to associate in public and in private with others of like mind, the right "not to be deprived of life, liberty and property without due process of law," and the right to be free from self-incrimination—in short, a Constitution which provides for a right to personal privacy.

And yet we are familiar with a host of cases in which each of these constitutional guarantees has been broken, because of a devotion to investigative techniques which abhor constitutional limitation. Have we not seen a number of citizens, some prominent and some publicly unknown, "investigated" and "documented" because of group-affiliations which someone has deemed "unacceptable" or "suspicious"? How many times has an individual accused of having committed a crime been found innocent of all charges, but the fact of his having been charged placed "on file" and allowed to plague him for the rest of his life?

Too often, errors in files and in printouts cannot be corrected because of the limited access given to the very individuals who are being investigated and discussed. Credit reporting has created a massive network of information, often faulty, that is not corrected and which continues to libel individuals without their knowledge.

The probability of an unregulated network of information being mislabeled and misdirected against an individual is a substantial danger in our computerized society. This afternoon applaud the efforts of my colleagues who realize that limits have to be set, and a balance struck in the interest of both law enforcement and constitutional, democratic government.

Mr. QUIE. Mr. Speaker, one of the biggest reasons for the United States breaking away from England was the right of privacy. Again, we find as we near the Bicentennial of the United States, the private citizen's right of privacy is again being eroded. It has confronted us in criminal matters, credit information distribution and computer data collection. It is no longer just a question of whether a man is entitled to privacy in his home, but whether his thoughts and actions will be placed on the public record against his wishes or without his knowledge.

The Bill of Rights and other parts of our Constitution preserve for each person a number of rights. Considered together, the basis for many of these is a right of privacy—it is the philosophical basis for freedom of speech, assembly, and religion and for protection from unreasonable searches and seizures and self-incrimination. Moreover, the 9th amendment states that the enumeration of rights in the Constitution is "not to be construed to deny or disparage other rights retained by the people," and by means of the due process clauses of the 5th and 14th amendments, each person is entitled to an explanation as well as an opportunity to explain in any confrontation with a Federal or State government or entity.

While an individual may not be put on the rack to make him inform on himself, this has not kept the Government and private associations from collecting

data on him. My concern is that it is without his consent or knowledge, may be inaccurate, and its uses are unknown. The fact is, such great potential exists or is being realized in the collection, storage, and recall and dissemination of computer data on individuals, that an individual's life may be reviewed in a matter of minutes without his knowledge or explantion.

Data collection and dissemination is not confined to credit ratings and reports or income tax returns, but includes many other areas of life where information is collected. Monthly, the Privacy Report, published by the American Civil Liberties Union Foundation, details these other instances. The March 1974 Privacy Report carried an item that the social security numbers of professors at the State University College at Geneseo, N.Y., will be recorded with the courses they teach so that the university system can automatically correlate data on every teacher's course load, enrollment, salary, rank, and class hours. Students then discovered that they were not allowed to see the files kept on them by the student placement office even though they felt that they had a right to see their own files.

And, this past weekend, a popular Sunday supplement—Parade, March 31, 1974—ran an article on the invasion of privacy in our public schools. The following is one illustration of several in the article:

"A parent is informed by a guidance counselor, about to write a college recommendation for her son, that his "psychological" file labeled him a possible schizophrenic back in elementary school."

In this case, the mother was not aware such a file existed.

The magazine reported it is becoming more and more common for schools to collect "soft data on children and their parents and allow access to this data to many persons, but not the parents or the child. The article lists instances of reports on parents' attitudes and activities and childen's behavior and psychology. The danger is that these reports are subjective comments, recorded without challenge, and possibly stigmatizing the child or his family with the broadcast ramifications.

It is time for Congress to act. It must act to define a right of privacy, and it must assess each other piece of legislation with due regard to that right. In the case of the Federal Government, Congress should limit the collection of data, open files to the individual concerned, and allow the individual an opportunity to comment and have his comments become a part of that file. With regard to the States and their agencies, Congress should assess its aid programs to see that Federal funds are not spent in contravention of a policy of a right to privacy or even that the States and its agencies must act positively with regard to such a right before qualifying for Federal aid. In the case of private information collectors, Congress should open all files to the individual concerned, when that file may be used by others than the collector, and allow the individual the opportunity to comment and have his comments become part of the file. In all cases, the individual must be given some control over the dissemination of information about him.

Ms. Abzug. Mr. Speaker, I wish to compliment my colleagues, Mr. Koch, Mr. Goldwater, Mr. Moorhead, Mr. Horton, Mr. Edwards, and Mr. Kemp, for taking this special order to express the congressional commitment to privacy. The field of privacy is a broad one, relating as it does to an individual's control over all knowledge or data about himself whether such data be collected by the private sector or by Government agencies, by the military branch or in connection with criminal investigations. As has been pointed out, there have already been over a hundred different bills and resolutions introduced in the House in the privacy field during this Congress and our approach has been somewhat fragmented. I have today introduced a bill which strives to cover some of the essentials in this area and which I hope will be useful. Although my bill is narrow in scope in that it attempts to deal only with an individual's control over information collected about himself by Federal agencies, the remedies provided are broad—broad enough to assure the individual citizen of adequate protection in the collection, maintenance, and disclosure of data about himself.

Several of us here today have taken an active role in attempting to protect the individual citizen from violations of privacy and other individual rights perpetrated by the Government in the guise of its legitimate functions. This was long before privacy received the imprimatur of a formal group within the Domestic Council, headed by Vice President Gerald Ford, long before the protection of privacy became a "fashionable" legislative subject. In the mid-sixties, a few

voices in the Congress spoke out, but their warnings seemed to fall on deaf ears. Books by law professors Alan Westin and Arthur Miller widened the discussion.

In July 1973, the report of the Secretary's Advisory Committee on Automated Personnel Data Systems, Records, Computers, and the Rights of Citizens was issued and has dominated the field. It is a most compelling document and should form a basis for any legislation in this field. Finally, and most recently, we had official administration recognition of the dangers of invasion of privacy when President Nixon created his Committee on the Right of Privacy last February.

Among my colleagues who have worked long and hard in the privacy field is one of the cosponsors of today's special order, Mr. Koch, who has introduced several bills dealing with persons' access to files maintained by Government agencies. Preliminary hearings on two of these bills—H.R. 12206 and H.R. 12207—were held before the Foreign Operations and Government Information Subcommittee of the Government Operations Committee, of which I am a member, last February. During these hearings, several witnesses made suggestions, many of which were agreed to by Mr. Koch, of ways to provide additional safeguards to individuals in today's computerized, mechanized, and highly bureacratized Federal Government. Although the more limited approach reflected in these bills may have been viewed as the optimum to be accomplished only a short while ago, I feel that the day has come when a strong privacy bill can be enacted. One need only look at the list of supporters of this special order to see that concern for privacy cuts across all partisan and ideological lines. We should certainly be able to rally bipartisan support for a stronger, more precise bill which will afford adequate protection and remedies to individuals regarding information collected, maintained, and disclosed by Federal Government agencies.

Having long taken an active role in this area and feeling strongly about the need to protect individuals against violations of their privacy, I have drafted a bill which incorporates many of the best provisions of Mr. Koch's bills with others pending in the House, including Mr. Goldwater's bill, H.R. 11275, pending in the Judiciary Committee. Althonugh the scope of my bill is similar to Mr. Koch's, I have attempted to adopt the suggestions made in discussions before our subcommittee in order to provide wider protection to the individual in the collection, maintenance, and use of personal data, including safeguards against improper alteration or disclosure of such information. Thus, my proposal attempts to place some limitations on the kinds of information collected by Government agencies. The root of the problem lies in the collection process—in the amount of unverified, irrelevant, and often erroneous data that finds its way into individuals' files. Further, by providing individuals' with access to their own files and the opportunity to correct such files by the removal of both irrelevant and erroneous material, limitations are imposed on the maintenance of data. Third, the use made of such data is restricted by requiring individuals' consent before disclosure of their files or, where disclosure may be required by law, prior notification and an opportunity to object. Beyond that, my proposal would define exemptions from its coverage in much more precise and enforceable terms.

This is one area where I feel that most proposed privacy legislation has been grossly deficient—in providing loosely defined exemptions for criminal justice information and for national security. First, let me discuss the criminal justice system. My legislation specifically includes records in this area, because I believe we cannot make an exception of one of the most abused areas and then expect the people of this country to feel we have produced a serious piece of legislation.

The only exception I have made in this area is "records that have been opened and are being used in pursuit of an active criminal prosecution." Those records will not be disclosed to the individual, but unlike other bills, that will be the limit of such nondisclosures. I believe the time has come to recognize that there are "datamaniacs" abounding in law enforcement agencies, people who collect everything about everybody with little or no thought as to the information's possible use in a constructive way. Once this information has been collected, it takes on a validity by the mere fact that it exists in law enforcement files and puffs out a cloud of suspicion in the minds of people who collect it or review it later. The mystique of "law and order" endows such dubious data with a respectability far greater than its sources should create.

If "law and order" is discredited as a precondition for secrecy, similarly the phrase "national security" should no longer be used as a pretence to excuse violations of privacy. Thus, my bill limits the national security exception to three areas—where disclosure would endanger the active military plans or deployment of U.S. forces, reveal details about current military technology or weaponry, or

endanger the life of any person engaged in foreign intelligence activities of the United States. Actions taken in the past under the color of national security have, in my judgment, created a clear and present danger to a legitimate concept of national security and I do not believe it is intelligent to add more yards to the national security blanket so beloved by people in authority.

Others have suggested quite properly that a Federal Privacy Board could assure that the sensible information standards and practices which have been praised so widely on the floor today are followed within the executive branch. Enforcement mechanisms are essential to anything which presumes to call itself legislation.

We must fix the responsibility for enforcing the law and order we seek to impose in a period so fraught with lawlessness and disorder. I support a privacy board for that primary purpose, but I also hope that we will see fit to empower it with sufficient authority to have a cleansing effect throughout the entire privacy area.

In the beginning, its first task will be to publicize the existence of data banks containing personal information. "Records, Computers, and the Rights of Citizens" and Mr. Goldwater's bill both have this ringing sentence which I have used in my own bill:

"There must be no personal data recordkeeping system whose very existence is secret and there must be a way for an individual to find out what information about him is in a record and how it is used."

In order to make that declaration a reality, we cannot rely on the individual agencies themselves, nor can we depend on an Attorney General to ferret out all the systems. Only an independent and strong privacy board can fulfill this educational task.

One of the great obstacles to the success of the privacy campaign thus far has been the lamentable fact that nowhere, either in the Congress or in the executive, or in the society at large, has there been a single group whose sole function has been the preservation of privacy. A Federal Privacy Board with jurisdiction to consider how information is collected in the first place as well as to control its centralization and dissemination could provide a focus for all those truly interested in making a reality of the Bill of Rights.

Mr. FASCELL. Mr. Speaker, it is a privilege to join our colleagues today in this discussion of the congressional commitment to privacy.

In recent years much use has been made of the somewhat elusive phrase—"quality of life." There is a very improtant aspect of the "quality of life" concept that has been threatened increasingly and which must have our attention. I speak of each citizen's right to protect his individuality—his privacy.

We are all seriously concerned with the erosion of public confidence in elected and appointed officials. Government seems somehow to have gotten away from the peole, to have grown so large that individuals can no longer identify with it. Citizens feel, I believe, that they have no access to Government, that Government acts arbitrarily, and that when Government so acts they have no manageable or easily available means to effectively respond or appeal.

But as Government has become seemingly less accessible to individuals, individuals have, so to speak, become much more accessible to Government.

It has been common knowledge for some time that various agencies of Government maintain files on individual citizens. We have all been shocked, however, to learn the extent of such recordkeeping and the manner in which the records have been used.

The growing computer capability—the ability to feed vast amounts of information into computers, store it, and retrieve it almost instantaneously—has vastly increased the potential for misuse of Government information. Prof. Arthur Miller, of George Washington University's National Law Center, wrote in a recent article on privacy that the technological ability to collect and disseminate information is virtually unlimited. Professor Miller wrote:

"What is technologically possible will be done."

While I do not necessarily agree with his conclusions, I regret that his assessment of the use of our technical ability is probably accurate unless we enact safeguards and controls.

At a time when public confidence is waning in a government which seems to be unapproaching, and when a growing technological capability exists for invading the lives of individuals, action must be taken to give individuals the right and the means to find out what files the Government maintains regarding them and to review and supplement them.

The very existence of vast Government records on individuals is alarming enough. The least we can do is provide adequate statutory safeguards, so that those records will not be misused.

I have joined our colleague Congressman Ed Koch in sponsoring the Federal Privacy Act, legislation which I feel would make a significant step toward providing the necessary safeguards for the use of Government files. The bill would do much, I believe, to protect the individual's interests.

Eessentially the bill would provide the following:

"Require each agency that maintains records to notify persons when their records are to be disclosed to any other agency or to any person not employed by the agency maintaining the record;

"Permit any person to inspect his own record and have copies made at his expense;

"Permit any person to supplement the information contained in his record by the addition of any document or writing of reasonable length;

"Require that erroneous information brought to the attention of the agency be removed from the record and that each agency and person to whom the erroneous material has previously been transferred be notified;

"Restrict access to the records to those in the agency who must examine the record to perform their job; and

"Require the record holding agency to keep as accurate record of the names and addresses of all persons to whom any information has been transmitted."

While this bill may not solve all the problems visited upon our citizens by the Federal bureaucracy, I believe it would be a large step in the right direction. Allowing the people to see information concerning themselves and upon which decisions affecting their lives will be made will help restore faith in our democracy. No longer would individuals be uncertain just what information was utilized and by whom when they request agency action in a matter important to them. And no longer would they be penalized by the damaging effects of erroneous information.

People would again believe themselves to be more than just a number in an agency computer when they see that they must be consulted in matters of personal importance. The individual would have an input and could insure that his records are accurate and up to date.

There are a number of other legislative proposals pending in the House which would also make important steps toward insuring individual privacy and liberty. But as the sponsors of this discussion have pointed out, the fragmented approach to congressional action may have slowed progress in enacting broad-purpose legislation.

I commend the sponsors of this debate, and hope that it will lead to cohesive action by the House to enact effective controls over the collection and use of information by Government and eliminate the continued risk of unwarranted and unacceptable invasions of privacy.

Mrs. SULLIVAN. Mr. Speaker, I am happy to join the gentleman from New York (Mr. Koch) a member of the Subcommittee on Consumer Affairs, in this discussion of the worrisome and frequently frightening aspects of the widening scope of invasion of privacy of the American people. As our population has increased and become more urbanized, and the management levels of business enterprises and of Government agencies become more and more separated from the individuals with whom their institutions deal—separated by increasing layers of public and private bureaucratics—the citizen becomes a disembodied social security number, credit card number, taxpayers' account number, and name and address on a computerized mailing list. He seldom has any personal relationship with the owner of any business with which he deals; he has little or no contact with any responsible official in a bank with which he has his account—in fact he may bank by mail and withdraw by check and never set foot in the bank; although he may have a mortgage with a mutual savings and loan association and thus be a member of the association, the chances are that he never attends an annual meeting of the association or attemps to take any part in the operations of the institution; on the job he may be known only by his immediate supervisors and the limited number of workers with whom he comes in daily contact.

Although the average urbanized citizen may feel that he moves in a kind of general anonymity, except among his friends and immediate neighbors and co-workers and fellow club members and so on, there is a great deal known about him by a great many people he does not know and who have no personal interest in him whatsoever. These strangers, who may have an occasional business or pro-

fessional interest in some aspect of his life, know, or can find out quickly and economically, virtually all there is to learn about his economic status, his credit worthiness, his reliability, integrity, general reputation, mode of living, personal habits, military record, taxpaying experience, political inclination, religious affiliation, police record, medical history, and a great many other things about him that he may or may not be willing to volunteer to perfect stranger without knowing how or when that information might be used. And often the information is slanted, of false, or a least incomplete and misleading.

FROM KINDERGARTEN TO THE GRAVE

The March 31 edition of Parade distributed with many Sunday newspapers gave us all something of a shock when it described the records being accumulated in the schools of this country about children from elementary school on up—teacher descriptions or criticisms of the character or emotional stability or abilities of youngsters which, in many instances are withheld from parents but could be used to damage the child in later years. Apparently, one's life becomes an open book from kindergarten to the grave.

Ideally, all of us should be empowered to protect our privacy as completely as we would like—to have control over the information about us we wish to allow anyone to have. As a people, however, we have surrendered by law—by laws written by the democratically elected representatives of the people—many of our inherent rights of privacy. For instance the 16th amendment to the Constitution provides the authority under which the Government compels us all to report every cent of our income and pay taxes thereon. We are compelled by law to answer census questions every 10 years. In applying for certain benefits available from the Government, such as food stamps for low-income families, citizens must divulge the most intimate of financial details down to the cash value of life insurance. In addition, in applying for employment, insurance, or credit from any public or private source the individual is called upon to lay bare facts about himself or herself that he or she would prefer be held confidential by those to whom the information is being given. Eventually, however, much if not most of this information finds its way into a computer somewhere where it is stored and held for the instant retrieval for the information of anyone who can establish a so-called legitimate business interest in having the information. These may or may not be people with whom the individual is consciously interested in doing any business.

THE START OF LEGISLATIVE PROTECTIONS

The proliferation of data banks in and out of government have been a source of deep concern to numerous committees and Members of Congress over the years. It took concrete legislative form for the first time early in 1968 when Congressman Clement Zablocki, of Wisconsin, offered an amendment to the truth in lending title of the Consumer Credit Protection Act, as it was being debated on the House floor on January 31 of that year, a provision which would have limited and regulated the kind of personal information compiled and sold for a fee by credit bureaus. The Zablocki amendment raised many questions which could not be answered satisfactorily on the House floor when it was offered that day, and it was defeated. But it was revived by Mr. Zablocki in more carefully defined legislative form in the next Congress and became the nucleus of what is now the Fair Credit Reporting Act of 1970—title VI of Public Law 91-508; which created a new title VI to the Consumer Credit Protection Act of 1968.

The Zablocki bill itself was never acted on in the House in the 91st Congress, nor was a much more comprehensive bill which I introduced in that Congress as chairman of the Subcommittee on Consumer Affairs and on which we held hearings in the subcommittee. Unfortunately when it came time to act on my bill in the subcommittee during the final weeks of the 91st Congress, we were never able to get a quorum of the subcommittee to begin markup sessions. The revised legislation was extremely controversial, and that fact may or may not have been a factor in our inability to get a quorum for markup sessions.

HOW THE FAIR CREDIT REPORTING ACT WAS ENACTED

In the meantime, however, the Senate had passed a Fair Credit Reporting Act modeled pretty much along the lines of Congressman Zablocki's bill and then tacked it on as a Senate rider to a House bill dealing with bank secrecy.

That is how we were able to get into conference on the Fair Credit Reporting Act before the 91st Congress adjourned. The Demorcatic members of the House Conference Committee, Representatives Patman, Barrett, Sullivan, and Reuss, proposed a series of strengthening amendments to the Senate-passed measure intended to bring it more into conformance with the bill I had introduced in the House and on which our hearings were conducted in the subcommitte. Some of those amendments were accepted by the Senate conferees and some were not. Looking back on that conference committee in 1970, I think it is now clear that if the House conferees had prevailed in conference on the disputed areas of this legislation, most of the criticisms now being voiced about the Fair Credit Reporting Act would not now be made.

The Fair Credit Reporting Act has accomplished a great deal of good in enabling individuals to find out the kind of information which is being circulated about them by credit bureaus and to require correction of erroneous or incomplete information. It requires the removal of obsolete information—in most instances, information more than 7 years old. It limits the purposes for which personal data can be made available. It provides for recourse by the consumer who has been damaged by credit bureau negligence.

DEFICIENCIES IN THE STATUTE

The most glaring deficiency in the Fair Credit Reporting Act is one which we fought over long and hard in conference, but the original Senate provision prevailed. It provides that a consumer may obtain from the credit bureau the "nature and substance of all information" in the consumer's file. The House conferees offered an amendment to delete the words "nature and substance of" so as to permit the consumer to examine all the information in his file, except for specified items such as medical data or the sources of investigative information.

It is in the area of investigative consumer reporting, where the credit investigators interview neighbors, former employers, ex-wives or ex-husbands, or anyone they can find who might be able to provide adverse information about an individual's intimately personal life, that the limitations on the consumer's right to see all of the information in his file lead to suspicion that the full file is not being disclosed. The Federal Trade Commission's efforts to check compliance with the disclosure requirements of the act have been stymied, at least temporarily, by a ruling of the district court for the District of Columbia that the FTC itself cannot have access to the complaining consumer's file.

In my mind, the other area of most serious shortcoming in the act is its failure to provide the FTC with authority to issue regulations which would have the force and effect of law in setting out compliance procedures, power such as the Federal Reserve Board has under the Truth in Lending Act to issue binding regulations, as contained in the Fed's regulation Z.

TESTIMONY BY SHELDON FELDMAN OF THE FIC

Mr. Speaker, because of its potential inmportance in protecting the consumer's rights of privacy, it is essential that we strengthen the Fair Credit Reporting Act to carry out more of the objectives the House conferees tried to write into the law nearly 4 years ago.

Mr. GOLDWATER. Mr. Speaker, in conclusion of this special order, let me just say that we recognize this question of privacy, not as a partisan effort or a partisan issue, because it is a problem that plagues all of us, whether we be Republican or Democrat, liberal or conservative. It is a peoples' problem, whether they are children or adults.

It is one that is long overdue, long in coming, for us to examine where we have come and how we got where we are today, and to bring those safeguards into the systems that were created with all good intentions to record and file information on our individual persons.

The most secret thing we have is our liberty in personality. This is a privilege which we should enjoy and protect, and one which this Congress, this body, should make a full commitment to protecting and establishing the proper safeguards in all types of legislation that we pass here on the floor.

Mr. Speaker, I commend my colleagues who have joined in sponsoring this special order today, and those who have contributed for the RECORD in this congressional commitment on privacy.

[From the Congressional Record, House, Apr. 4, 1974]

Dr. Willis H. Ware

The Speaker pro tempore. Under a previous order of the House, the gentleman from California (Mr. Goldwater) is recognized for 10 minutes.

Mr. Goldwater. Mr. Speaker, a pillar of integrity and learned in information technology is Dr. Willis H. Ware, currently on the research staff of the Rand Corp. and recently chairman of the Secretary's—DHEW—Advisory Committee on Automated Personal Data Systems.

The Nation was most fortunate to have his able services during the preparation of the report and recommendations of this advisory committee widely considered a landmark in its field. I recently read his essay in the annual report of the Rand Corp. for 1973, entitled "Databanks, Privacy and Society." A succinct excerpt immediately caught my attention:

". . . in the balance of power between a citizen and the totality of systems that keep records about him, he is at a significant disadvantage."

Mr. Speaker, the basic ingredients of my legislation on fair personal information practices and limiting the use of the social security number are embodied in this presentation. I believe we must give strong legal rights to individuals in order that they can have access to their records. We must reestablish the pluralistic concept of our society that separates our relationships with our bank, our doctor, and our Government or shopkeeper. The notion that some master dossier is to be built from all our daily relationships requiring information giving is growing more popular today.

I salute Dr. Ware and those at Rand and on the DHEW Advisory Committee who have reawakened some elements very true to America. May they continue as important contributors to our social policy choices.

At this point, Mr. Speaker, I request to include Dr. Ware's essay in the Record.

[The essay follows:]

[Source: Rand Corp., Santa Monica, Calif., 1973]

Data Banks, Privacy, and Society

(By Willis H. Ware)

Computer technology provides society with the tool it needs to accommodate growing information requirements. It lets us keep the records we have to keep, economically and efficiently. But the computer-based automated file can also work against us. The information in computer systems can be valuable and thus subverted for inappropriate purposes. Because of this vulnerability, automated data systems add a new dimension to the problem of personal privacy, as well as provide opportunity for embezzlement, blackmail, and other fraudulent schemes. Our essential tool could become a major societal threat unless we provide effective safeguards to protect personal information in automated files and those to whom it pertains.

The attitude of the public with regard to personal information has changed in recent years. We are becoming increasingly aware of data files and the information they contain about us.

To some data systems we provide personal information voluntarily. We do this in exchange for some benefit, privilege, or opportunity: we want to make credit-card purchases, obtain loans, write checks, get a passport, apply for a job. Some information we provide because it is required by law: we participate in the census or fill out questionnaires for military service. Sometimes we provide information inadvertently: we are in an accident that involves a police record.

We provide considerable information because we ask for services from government. We want educational assistance, unemployment support, housing allowance, or care for the older segment of the population. Congress, in turn, insists on strict accountability of public assistance programs and on evaluation of the success of such undertakings; this requires personal records and computer processing. The more extensively we and the government interact, the more extensive must be the records that need to be compiled and maintained by computer.

INFORMATION NEEDS OF GOVERNMENT

As our population increase and our society becomes more complex, and as the government enlarges its range of services, the need for personal information grows. The federal government, for example, needs extensive information in order to formulate new legislation, to adopt sound fiscal and tax policies, for entitlement decisions with regard to public assistance programs, to estimate the consequences of a possible decision, and to generally conduct the affairs of the country.

In the face of increased demand for natural resources—and many man-made resources—comprehensive planning becomes crucial at all levels of government. To adequately balance quantity and demand for land, energy, water, highways, etc., government regulation and intervention are required. Local governments need information to regulate land use, and to plan sewage and water facilities, transportation, and many other public services.

Industry gathers much personal information in order to assemble and maintain the records that are required in an era of intricate labor relations, widespread union practices, pension and insurance plans, state and federal tax withholding, and other regulatory and legal restrictions. Social research is also increasing, and along with it social experimentation, so that more information about people, their behavior, and their habits must be gathered. Thus, there exist numerous automated files containing extensive personal information about all of us.

ACCESSIBILITY OF PERSONAL INFORMATION

For whatever reason we furnish information about ourselves, we implicitly tend to assume that it will be used only in our best interest and solely for purpose for which it is furnished. Thus it comes as a surprise when we find that the information we have provided for one purpose is being used for a different one. As a result of personal data submitted for a driving license, for example, we find ourselves on a mailing list and inundated with advertising literature.

While much personal information in automated files is anonymous, describing in a statistical way some characteristic segment of the poulation, there is also much that is identifiable in order to permit decisions to be made based on a person's record. Given our mobility in residence and employment, many organizations find it expedient to exchange data or to transport information about an individaul from one place to another. Thus the automated record system tends to concetrate information about people in one place and to provide ready accessibility to it for a wide group of users. Moreover, automated systems can, in principle, exchange data, automatically with one another and so broaden the exposure of personal information. Such linking of files, when it occurs, enlarges the volume of data available to any one inquirer.

Of the many files containing personal, private information, a considerable number are at government level: census data, social security records, Internal Revenue Service tax records, various research collections in the social and life sciences, etc. Some are in the financial industry; bank account records, savings and loan records, stock investment records, credit records. Many relate to health care, such as hospital, medical, or psychiatric records. A few have been collected by the recreational and leisure-time industry in the course of making reservations and travel plans. Those accumulated by educational institutions include a complete, detailed account of performance in high school and college.

SOCIAL SECURITY NUMBERS AS IDENTIFIERS

If the file is for a local purpose, it may be sufficient to identify the individual by his name and address. Often some secondary identification is included; the mother's maiden name is one traditional exemaple. In many instances, federal statutes require that a person's social security number be given as an authenticator of his identity; financial institutions, for instance, are legally required to obtain it.

Federal statutes or requilations will, in some cases, authorize the exchange of information among data banks. The Internal Revenue Service, for example, regularly exchanges data with state tax-collection agencies; and in so doing, ensures that identity is preserved and records are kept straight by means of the social security number. In other cases, an administrative action will stipulate that

social security numbers must be obtained. They are required by the Department of Motor Vehicles in some states, for example. Occasionally, social security numbers are secured for no particular purpose other than as a hedge against an unknown future need. Some educational organizations use them as student identifiers.

Unfortunately, the growing number of automated files in which a record about an individual includes his social security number implicitly encourages the exchange of information; it also serves as a key for combining information from several sources. Sometimes, exchange of data is facilitated by freedom-of-information acts at both federal and state levels, because these acts require that public information be provided to any requester. A person who finds himself in a file considered to be public information has no effective control over how his information will be used.

While linkage among information systems is undoubtedly not yet so widespread as to be considered at the critical level, many factors suggest that the situation is likely to develop: the remote-access computers systems that service geographically distributed users; the awareness by a manager or an official that information from some other sources will help him do his job better; recognition by a researcher that combination of files will give him more insight into his problems; and the economic efficiency of combining several small information systems into a large one serving many classes of users.

CONTROL OF PERSONAL RECORDS

With this growing awareness that automated files pose a real threat to personal privacy, we are becoming more senstitive to the misuse of personal information, and are willing to complain about it. Our complaint may simply be the result of a personal annoyance—a dunning letter received because a paid bill has not been accurately posted to the correct account; but the complaint can be much more serious. Because of incomplete or erroneous information in an automated file, we may suffer a damaged reputation, loss of financial status or position in the community, the denial of credit, the loss of a job, or improper arrest.

Public concern over the invasion of personal privacy may well rest more on a sense of having lost control—of not knowing when information freely given for one purpose will be used for another—than on the feeling of being surrounded by a data-hungry environment. We feel a need to be guaranteed that personal, identifiable records will be used in way over which we have some control—and that we have a mechanism to seek recourse in case we should sustain harm if they are improperly used.

The Constitution of the United States does not *specifically* provide for a right of personal privacy. Justice Brandeis, dissenting in the case of *Olmstead* v. *the United States* (198), first suggested that personal privacy is implied in the Constitution. A continuing series of judicial interpretations have cumulatively created the right of privacy. The legal basis for these judgments includes the first amendment guarantee of free speech, press, assembly, and religion; the third amendment prohibition against quartering soldiers in private homes; the fourth amendment right to security from unreasonable search and seizure; the fifth amendment right against compulsory self-incrimination; and the ninth amendment guarantee of other unenumerated rights retained by the people.

Recent Supreme Court decisions have declared the right of personal privacy as the basis for protecting such freedoms of an individual as the practice of contraception or the reading of pornography in the home. Unlike the United States, for other countries—Canada, for example—have not developed a constitutional or legal basis for extending personal privacy to its citizens.

From the standpoint of the individual citizen, he is generally unaware that information about himself is being disseminated without his approval; in most instances he is powerless to stop it even if he should discover it. Since large information systems are a relatively recent development in a technical and operational sense, one can expect to find inadequacies in their designs or incomplete operational practices, either of which can be manipulated to steal information, or can result in inadvertent or malicious leakage of information to someone not authorized to have it. Furthermore, information in data banks is usually not protected against legal process. While specific legislation does sometimes protect information in automated files, or authorizes a government official to extend protection as he sees fit, by and large, the bulk of information in such files is subject to confiscation through administrative or legal subpoena or through other court-directed seizure.

HOW TO ACHIEVE PROPER BALANCE?

Thus the exploitation of computer and communication technology in modern recordkeeping systems highlights the central contention between the need of government and business organizations to have personal information for efficient planning and operation and the need of the individual to have control over the way in which information about himself is used. How can we achieve a more satisfactory balance?

There are actually two quite different issues involved. One is the technical problem of designing and implementing an automated information system that will safeguard the data it contains. A properly designed system will not inadvertently leak information, and it will be physically protected against pilfering, thievery, and infiltration. It will deliver information only to users authorized to have it.

The other issue is the much more difficult one of controlling what personal information should be collected in the first place, of determining who shall have access to it and for what purpose, and of giving the individual more control over information about himself. Unlike the control exercised over national security information, there is no classification scheme established by law or executive order for labeling personal information as "sensitive," "nonsensitive," or "ultrasensitive"; nor are there any government-wide guidelines for establishing who may have access to it. Thus, the rules and regulations governing dissemination of personal information from a file tend to be made by the individual or organization that collects the data and owns the file. In many instances, there are no established practices to serve as a model for good procedure. In the particular case of consumer credit reference systems, the Fair Credit Reporting Act does impose limited constraints; for example, provision is made for the individual to inspect his file and to correct it.

SOME SUGGESTIONS FOR SOLVING THE PROBLEM

In solving the technical problem, physical protection, computer hardware and software safeguards, communication security safeguards, and a general management-procedural overlay are collectively necessary to provide the overall protection needed. In all of these areas, the requirement of the defense community to protect classified information is a driving force for research, new system designs, and general progress toward an eventual solution. Fortunately, many of these same safeguards are needed in any computer system that shares its resources among many users—that is, the time-shared computer system—and to this end the general advance of the computer industry will help to provide the technical basis needed.

In solving the problem of restricting the collection of personal information, of controlling its dissemination, of carefully specifying what use may be made of it, and of affording the individual greater participation in the dissemination of his personal information, various suggestions have been made but none have been generally implemented. To improve the care with which recordkeeping systems are designed and operated, one proposal is to certify computer programmers and system designers. This action would assuredly be a useful one; but unlike the older engineering fields, the computer field does not yet have a well-established body of preferred practice upon which to draw. Thus, while certification would be a helpful step, it would put the responsibility for a properly designed and controlled record system in the wrong place. The responsibility should be assumed by the organization that assembles the system, initiates its design, and operates it, not by the technician who implements it. While certification is a step in the right direction, it cannot of itself adequately solve the problem.

A second solution might be the ombudsman approach, which has been used for many years in Scandinavian countries. Basically, the ombudsman is a spokesman for an individual who has been harmed; he serves essentially as a communication channel between the person and the bureaucracy in matters of dispute. While the ombudsman concept is a useful third-party mechanism to facilitate resolution of argument, it is not a well-established mechanism in the United States nor can it function as a sufficiently strong force to be a solution for the entire problem of protecting personal privacy.

A third solution, one that attempts to deal with the problem through the established institutions and procedures of the country, would be to create by law a Code of Fair Information Practices in the spirit of already existing legis-

lation on labor practices. The intent of such a code would be to encourage ethical practices on the part of owners, designers, and operators of recordkeeping systems through legal deterrents. In this way it would be possible to specify how record systems should be organized and operated, how owners and operators should conduct their operations relative to the individuals about whom the information is held, what privileges and recourses the individual has, and to provide legal sanctions, both civil and criminal, that can be imposed for violations of the code.

The approach would have several advantages: It would exploit existing legal and judicial institutions and procedures. It would provide a self-adapting solution to the problem through the medium of court interpretation and judgment. It would require a minium of new bureaucratic functions. With regard to industry, the code would be handled by the General Counsel's office, as are fair labor practices, tax matters, and other industrial regulations.

Finally, a fourth possibility is to create a Federal Record System Commission, similar to the Federal Communications Commission or the Civil Aeronautics Board, that would serve as a regulatory body to license, register, and oversee the operation of all record systems dealing with personal information. However, this would entail the creation of substantial new bureaucratic structure and funding for it. More importantly, it would also be another instance of government intervention in the affairs of the people and industry. Given our national aversion to government intervention in business and industrial activities, and the fact that deterrent mechanisms have not yet been tried, a regulatory approach to the problem of recordkeeping appears to be one that should be kept in abeyance until other methods have failed and the need for it is clearly established.

A NUMBERED SOCIETY?

The Social Security Amendments Act of 1972 (P.L. 92–603) is suggestive of what can happen if no action is taken. The Act requires that a social security number be issued to all individuals, of any age, who are receiving public assistance from federal funds. It also authorizes, but does not require, the Secretary of Health, Education, and Welfare to take affirmative measures to assign social security numbers to all children on their initial entrance into school.

Should future legislative trend follow this precedent and gradually require all sectors of the population to have a social security number, then the United States will have reached the stage at which the population is fully numbered, a national population register can exist, and it will be technically feasible to maintain a lifetime dossier on each citizen. Other forces can lead to the same end. The introduction of the national birth certificate number will, for example, provide a unique lifetime identification for each citizen.

While a fully numbered population may not of itself be undesirable, the alarming fact is that we are drifting toward this state without public awareness that it is happening or public debate as to the possible consequences. The end result—that each of us will have a unique and permanent identifier—is not likely to happen from a well-engineered plan or deliberate intent. Rather, it will be the combined effect of many decisions, each made by someone doing his best job as he sees it at the time. It will be the cumulative effect of a variety of legislative steps, some unnoticed data collections, and a gradual widening of the operational scope of existing record systems due to economic pressures, coupled with a general ignorance that such events are occurring. In sum, a United States citizen could easily awaken one morning to find that he is uniquely identified for life and that all sorts of personal information are being collected under his label and widely disseminated for public and private use.

A NEED FOR ACTION

The issue of personal privacy has several major public-action aspects. It must be brought before the public, and kept there; the active support of consumer-oriented organizatins must be solicited to promote legislative measures; public participation in the debate about a fully numbered, registered society must be encouraged.

There are also researchable aspects. One is to examine the technical details of providing comprehensive safeguards for automated information systems. Another is to analyze the legal considerations involved in protecting the individual's right to privacy. Others are a study of the consequences of a fully numbered and registered society, a search for ways to provide comprehensive protection against abuse of personal information, and the development of means

for linking automated data systems while protecting the personal privacy of the data subjects.

Since automated information systems containing personal information are essential to today's complex society, it is imperative that solutions be found to the important problem of protecting our inherent right to privacy. There is certainly no question but that in the balance of power between a citizen and the totality of systems that keep records about him, he is at a significant disadvantage.

NOTE.—About the author: In the late 1940s Willis Ware was doing research under John von Neumann on an electronic digital computer—the first of the "Princeton-class" machines. After receiving his doctorate from Princeton in electrical engineering, Dr. Ware came to Rand in 1952 to work on the exploitation of computers for military, scientific, and civil problems. He headed Rand's Computer Sciences Department from 1964 to 1971, and is at present on the Corporate Research Staff. Among his many advisory appointments, he is chairman of the Air Force Scientific Advisory Board's Information Processing Panel and of the Secretary's (DHEW) Advisory Committee on Automated Personal Data Systems.)

[From the Congressional Record, House, Apr. 9, 1974]

CONGRESSIONAL COMMITMENT TO PRIVACY

The SPEAKER pro tempore. Under a previous order of the House, the gentleman from Ohio (Mr. GUYER) is recognized for 5 minutes.

Mr. GUYER. Mr. Speaker, this Congress would be remiss if the important issues of rights to personal privacy were not given thorough attention and legislation adopted to restore these badly eroded liberties.

The leadership of my colleague from California (Mr. Goldwater) is to be commended. He is following the footsteps of my distinguished predecessor Jackson E. Betts who made census reform a national issue. We are building on the concerns of a decade of congressional investigation into invasion of privacy. Regrettably, the record of accomplishment is far behind the rapidly growing advances in information technology. Thus, today's congressional commitment to privacy is a most propitious event.

My concern, Mr. Speaker, goes to the very essence of privacy—the right to one's self—the honorable right to participate or withdraw, to speak or elect to be silent. The right to supply personal information to a business or government with the assurance it will be properly maintained. The right to inspect that information, get a copy of it, to give permission before it is disseminated, to require its correction or distribution when errors occur or it is no longer needed. I am the sponsor of legislation to establish a Code of Fair Information Practices to accomplish these information rights for Americans.

Let me speak in support of a number of other bills sponsored by many of the 200 Congressmen already committeed to restoring privacy. Measures to allow parents to see their children's school records, limit mailing list distribution by Government agencies, reduce the scope of the census, stop requiring the social security number for every purpose, and strictly limit the use of personal income tax reports have my support.

Mr. Speaker, these are trying times for America. Times when public confidence in our institutions, including the Congress, is at a low level. One of the maladies causing such public attitudes is a hostility to the excesses of information collectors. Our American way of life is based on a balance of interest. Justice Samuel H. Hofstadter of the Supreme Court of New York stated this philosophy in a very impressive manner:

"In a democracy, we are concerned primarily with the relation of the individual to his government. And the maintenance of this overall relationship has greater importance than the isolated search for fact—or even justice—in any specific case."

These are my sentiments today.

[From the Congressional Record, Extensions of Remarks, Apr. 3, 1974]

INVASION OF PRIVACY

Mr. BAKER. Mr. Speaker, much concern has been voiced over the extent to which the privacy of the American citizen is being invaded. We see this in the

accumulation of personal data in computer banks, and this constitutes a threat to the privacy of every American citizen. For many years, Members of the House of Representatives have been concerned about the invasion of privacy of Americans.

Privacy is control over knowledge about oneself; it is not just the absence of information, but also the feeling of security of controlling the information available about ourselves. Americans must be assured that their private and personal lives will not be invaded through Government regulation. In the past, the spotlight has been focused on such issues as a proposal to create a Federal Statistical Data Center, lengthy debate over enactment of the Fair Credit Reporting Act, and the number, size, and pervasiveness of Federal data banks.

I want to express to my colleagues, Mr. Speaker, my very deep concern about privacy. This is a fundamental individual right recognized by everybody. We must be extremely careful to prevent individual liberties from slipping through our fingers and into the pot of Federal regulation.

[From the Congressional Record, Extensions of Remarks, Apr. 3, 1974]

Cumulative Student Records: A Potential Abuse of the Right to Privacy—Part I

Mr. Kemp. Mr. Speaker, the House engaged in an extensive colloquy this afternoon on the crucially important subject of more effectively assuring the individual's right to privacy—his right to be left alone—his right to be left alone. I was honored to be one of the principal cosponsors of that colloquy.

As I indicated in my earlier remarks this afternoon, there is growing concern over the potential abuse and improper disclosure of information now maintained and used by the public and private school systems throughout the country—extensive information on the social and economic background, attitudes and behavior, performance and ability, and health of pupils within those systems. The gentleman from California (Mr. Goldwater) placed a highly informative article, authored by Diane Divoky and appearing in last weekend's issue of Parade magazine, into the Record of our proceedings yesterday.

These student records contain—in addition to essential factual information relating to the actual education of the pupil—subjective evaluations made by teachers and other school officials, evaluations which are often unverified by supervisors or other instructors, and evaluations which often reflect the biases—intentionally or unintentionally—of the evaluators themselves.

Because the information stored in these elaborate systems follows the student as he or she goes through the learning process, from one teacher to another, from one school to another, often from one school system to another, and because this information is subjective and involves the most sensitive of data which can be ascertained about an individual, we must come to grips with the potential abuses which can arise from the disclosure of this information. In many, if not most instances, this information is available to such diverse entities as the military services, actual or potential employers, and institutions of higher learning.

There are some potential invasions of privacy which affect less than the whole population. This potential abuse of school records, however, affects everyone who has even gone to a public or private school—in other words, virtually all of us.

It is important that the Congress—in its sphere—and the State legislatures in their spheres—for education is primarily a matter of State and local jurisdiction—get a handle on this matter as soon as possible.

As I indicated in my earlier remarks, I have this matter under intense scrutiny, and I hope to be able to report to the House and to introduce appropriate remedial legislation at the earliest opportunity. This is certainly a matter which should not go without redress.

The Parade magazine article which was included in or proceedings by Mr. Goldwater was a condensation of an extensive article which appeared in the September 1973 edition of Learning, also authored by Diane Divoky. At this point in the Record, I insert the first half of that article:

[The article follows:]

CUMULATIVE RECORDS: ASSAULT ON PRIVACY

(By Diane Divoky)

It all started innocently enough back in the 1820s, when schools in New England began keeping registers of enrollment and attendance. In the 150-odd years since, the student record has grown to grotesque proportions. Like Frankenstein's monster, it now has the potential to destroy those it was created to protect.

Educators have constructed this monster in the name of efficiency and progress, adding a piece here and there, tinkering with new components, assuming all the while they were creating a manageable servant for school personnel. But what they failed to foresee was the swift development of modern communications technology and the widening employment of that technology by a social system increasingly bent in snooping.

The growth of the record into an all-inclusive dossier came in response to the increasing centralization and bureacratization of schools. Another conrtibuting factor was the emergence of education's ambitious goal of dealing with the "whole child." Out of that context grew such specific actions as the NEA's 1925 recommendation that health, guidance and psychological records be maintained for each pupil, and the American Council on Education's 1941 development of record forms that gave more attention to behavior descriptions and evaluation and less to hard data such as subjects and grades. By 1964, the U.S. Office of Education was listing eight major classifications of information to be collected and placed in the student record.

More recently, the Ohio Department of Education took a hard look at state laws requiring the keeping of such records sounded a note of warning: "When construed with other statutes which give school authorities wide discretionary power . . . it [is] obvious that schools may collect any kind of information they desire concerning pupils." Power of that magnitude, admonished guidelines for Ohio administrators, must be handled with great care and discretion.

The ultimate mushrooming of records may have been reached in the massive New York City school system—largest in the nation. There, the records required or recommended for each child involved, if nothing else, a staggering amount of book work. A typical, rainbow-hued student dossier in New York carries:

A buff-colored, cumulative, four-page record card that notes personal and social behavior, along with scholastic achievement, and is kept on file for 50 years;

A blue or green test data card on which all standardized test results and grade equivalents are kept, also for 50 years;

A white, four-page, chronological reading record;

A pupil's office card;

An emergency home-contact card;

A salmon-colored health record—one side for teachers, the other for the school nurse and doctor;

A dental-check card;

An audiometer screening-test report;

An articulation card, including teachers' recommendations for tracking in junior high school;

A teachers' anecdotal file on student behavior;

An office guidance record, comprised of counselors' evaluations of aptitude, behavior and personality characteristics;

A Bureau, of Child Guidance file that is regarded, though not always treated, as confidential, and includes reports to and from psychologists, psychiatrists, social workers, various public and private agencies, the courts and the police;

And all disciplinary referral cards.

In New York and elsewhere, as the records began to contain more detailed and varied information, they took on lives of their own, they became, somehow, more trustforthy and permanent than the quixotic people they represented. Read the cumulative folder of a student—131 IQ, strong language skills, musical talent, loss of vision in one eye, permissive home—and then meet the child, if he doesn't come on bright, articulate, humming a little and self-assured in sptie of a squint, something, one feels, must be wrong. And it's not likely the record will be blamed.

As the process of information collection in the schools snowballed—a few more forms for the guidance department, a few more facts for state agencies, another set of teacher commitments for anew tracking plan—almost no one stopped to

weigh the implications of recording so much hard and soft data about children and their families. There was little thought given to development of clear policies and practices by which student and parental rights of privacy might be balanced against the needs of the school and other social agencies to know, or to guarantee, that material contained in records was accurate and pertinent.

Thus, by 1970, almost any government agent could walking into a school, flash a badge and send a clerk scurrying to produce a file containing the psychiatric and medical records of a former student. It was unlikely that the student would even know about the intrusion into high private life. A mother could be cooly informed that she had *no right* to see the records that resulted in her child being transferred to a class for the mentally retarded. A father attending a routine parent-teacher conference about his outgoing son could discover in the boy's anecdotal record comments that he was "strangely introspective" in the third grade, "unnaturally interested in girls" in the fifth, and had developed "peculiar political ideas" by the time he was 12—judgments that the father could neither retroactively challenge nor explain.

Case histories such as these helped motivate sociologists David A. Goslin and Nancy Bordier of the Russell Sage Foundation to undertake a survey of of the record-keeping practices of 54 representative school districts. They found that the systems maintained as part of their permanent files widely varied information on students. Almost all kept informal teacher-made anecdotal records, special health data, notes on interviews with parents and students, correspondence from home, records of referrals, delinquency reports and other "high security" data. Nearly three fourths of them also kept personality ratings, samples of student work, diaries and autobiographies. One third recorded the race and religion of students, almost a half recorded students by nationality, and half kept photographs on the record forms. The research team also discovered that anyone from the school psychologist to a front-office clerk might be responsible for feeding information into the permanent file. (One interesting sidelight: The records were consistently little used by teachers and school staff, a finding that flew in the face of the official rationale that the dossiers were needed to guide teachers in their relations with individual students).

Goslin and Brodier also found that CIA and FBI agents had access to the entire student files in more than half the school systems, as did juvenile courts and health department officials. Local police had access to complete files in almost one third of the systems. But parents—those citizens with primary legal and moral responsibility for the child—had access to the entire files in fewer than 10 percent of the systems. Some superintendents reported that parents were denied access to their children's records even when they possessed the legal right to inspect them. "What is particularly significant," the researchers noted, "is the impression that school officials have strong reservations about giving parents very much information (other than routine grade reports and sometimes achievement-test scores) about the content of evaluations that are continually being made of their children."

As a follow-up to the Goslin-Bordier study, the Russell Sage Foundation convened in 1969 a group of prominent educators, lawyers and social scientists to consider ethical and legal aspects of school record keeping and to develop guidelines for the collection, maintenance and dissemination of these records. The conference report began: "There are clear indications . . . that current practices of schools and school personnel relating to the collection, maintenance, use and dissemination of information about pupils threaten a desirable balance between the individual's right to privacy and the school's stated need to know." It pointed to these abuses:

"Information about both pupils and their parents often collected by schools without the informed consent of either children or their parents. Where consent is obtained for the collection of information for one purpose, the same information is often used subsequently for other purposes.

"Pupils and parents typically have little or, at best, incomplete knowledge of what information about them is contained in school records and what use is made of this information by the school.

"Parental and pupil access to school records typically is limited by schools to the pupil's attendance and achievement record (including standardized achievement-test scores).

"The secrecy with which school records usually are maintained makes difficult any systematic assessments of the accuracy of information contained therein. Formal procedures permitting parental or pupil challenges of allegedly erroneous information do not exist. An unverified allegation of misconduct may therefore . . . become part of a pupil's permanent record.

"Procedures governing the periodic destruction of outdated or no longer useful information do not exist in most systems.

"Within many school systems, few provisions are made to protect school records from examination by unauthorized school personnel .

"Access to pupil records by nonschool personnel and representatives of outside agencies is, for the most part, handled on an ad hoc basis. Formal policies governing access by law-enforcement officials, the courts, potential employers, colleges, researchers and others do not exist in most school systems .

"Sensitive and intimate information collected in the course of teacher-pupil or counselor-pupil contacts is not protected from subpoena by formal authority in most states."

The report concluded that "these deficencies in record-keeping policies . . . constitute a serious threat to individual privacy in the United States." It suggested guidelines for record keeping based on these principles: (1) No information should be collected about students without the informed consent of parents and, in some cases, the child. (2) Information should be classified so that only the basic minimum of data appears on the permanent record card, while the rest is periodically reviewed and, if appropriate, destroyed. (3) Schools should establish procedures to verify the accuracy of all data maintained in their pupil records. (4) Parents should have full access to their child's records, including the right to challenge the accuracy of the information found therein. (5) No agency or persons other than school personnel who deal directly with the child concerned should have access to pupil data without parental or pupil permission (except in the case of a subpoena).

In 1972, the Sage Foundation tackled the subject once more and found that, in spite of the distribution of 100,000 copies of its guidelines, "the vast majority of schools in this country still do not have records policies which adequately protect the privacy of students and their parents."

The researchers also noted that good policy may not begin to solve record problems. In one school system visited by a researcher, a written policy was drawn up by a committee composed entirely of counselors. As a result, "the social worker thought it did not apply to her records, the mechanics teacher who had considerable informal contact with local employers thought that it only applied to formal requests for information handled by the registrar, and one of the principals regarded it as of the utmost importance to stay on good terms with local employers by telling them in detail of all the behavior problems potential employees had experienced while in school."

The Sage reports and guidelines helped fuel a growing national alarm about threats to privacy posed by our technological and bureaucratic society, and several educational groups subsequently took public positions insisting on the confidentiality of records. In 1971, the NEA, which 46 years before had urged more comphensive record keeping, approved the *Code of Student Rights and Responsibilities*, which asserts that the "Interest of the student must supersede all other purposes to which records might be put," and urges strict policies to protect the rights to privacy of students and parents. It suggested that junior high school students have joint control with their parents over their own records, and high school students, total control.

Recently, a few local school boards, notably those in Des Moines, Iowa, and Jefferson City, Missouri, have adopted regulations to safeguard records. Des Moines allows parents and students to see the records, asks written consent of them before any information is released to anyone else, and gives them the power to determine which records may never be released to anyone.

On the state level, Oregon has given parents the right to inspect the total record. Delaware grants students 14 years or older control over the release of information from their own records, and New Mexico guarantees any public school student the right to inspect his own record. Both New Mexico and Oregon have moved to keep records confidential from outsiders. Oregon law prohibits the release of records to anyone other than the parents and child. The New Mexico board of education policy statement says that "government investigative agencies as such have no inherent legal right to have access to student files and records," and the board bars them from access without the student's permission or a court order. New Hampshire prohibits schools from keeping records that "reflect the political activities or beliefs of students."

Some educators and parents, discouraged with waiting for legislators or school administrators to act, have sought to take the reins in their own hands. In San Francisco, a group of black teachers and counselors are working for the elimination of all records except for a small card of hard data. They argue that the image of a folder as some capacious pocket into which all sorts of alleged wrongdoings

and bad marks can be dropped has a bad psychological effect on students, that the folders consistently contain indefensible and gratuitious negative comments but little about the student's real educational ability, and that those biased comments are used authoritatively by the schools, particularly by guidance counselors, who see a folder as a kind of bible. "Black students' folders tend to be at least half an inch thicker than those of white children," one of the committee members said, "which tells you something about the child even before you open the folder."

The manner in which the thick folders of a group of junior high school students in Washington, D.C., were handled is now the basis of *Doe v. MacMillan*, a case before the U.S. Supreme Court. The suit was triggered when the House Committee for the District of Columbia, in preparation for its annual hearings on the D.C. schools, sent investigators out to gather up the cumulative records of students. Copies of actual test papers, disciplinary reports and evaluations—defamatory if not libelous materials—were reproduced with the students' names still on them. The report was then published by the committee's chairman, entered in the Congressional Record and circulated about the country. Parents sued the individual congressman as well as the school board, principal and teachers. Sovereign immunity protection in the District of Columbia complicated the case, but the U.S. Supreme Court recently ruled that the congressmen had no special immunity "from local laws protecting the good name or the reputation of the ordinary citizen" and remanded the case to the Court of Appeals for further action. Not coincidentally, the D.C. board of education established regulations for protection of records just as the complaint was filed.

The second half of the article from Learning will appear hereafter.

[From the Congressional Record, Extensions of Remarks, Apr. 3, 1974]

Cumulative Student Records: A Potential Abuse of the Right to Privacy—Part II

Mr. Kemp. Mr. Speaker, I include the second and concluding section of the article, "Cumulative Records: Assault on Privacy," by Dian Divoky, which appeared in the September 1973 issue of the magazine, Learning.

[The section follows:]

But even the best-intentioned policies don't guarantee ethical practices. A fair record policy in a suburban school district near Cleveland fell into disrepute when it was learned, that students were regularly given the job of transporting records from one building to another and were just as regularly snooping on each other.

A California law passed in 1959 assures parents of the right to inspect their children's cumulative records, but local school official frequently refuse access or fail to inform them of the privilege.

California's state education code also forbids school employees from giving out personal information about pupils to anyone except specified officials. That didn't stop one district administrator, acting in advance of a school board hearing into the suspension of a student, from publicly, announcing that the boy had been guilty of "serious violation of manners, morals and discipline." Three years later, the courts found that the public statement was based on nothing more than allegations of the school superintendent, and the student was awarded damages.

So while scattered improvements in the national picture have indeed occurred, school records continue to provide an easy route for invasion of privacy. Perhaps the worse abuses of school record keeping in America occur, despite well-established guidelines to the contrary, in the country's biggest and reputedly most liberal city, New York.

During the months that the author served on the New York City board of education's committee to revise student records (as chairman of the subcommittee on safeguarding and dissemination), these incidents occurred:

A secretary at a private tutoring agency, calls a public junior high school to inquire about a child's reading level. The principal opens the child's record and gratuitously informs the unseen caller that the child has a history of bedwetting, his mother is an alcoholic, and a different man sleeps at the home every night. When the disclosures are reported to the board of education, the principal denies the incident and his immediate superiors back him up.

A teacher of a child entering a new school gets this summary of the student's past academic year: "A real sickie—absent, truant, stubborn and very dull. Is verbal only about outside, irrelevant facts. Can barely read (which was huge accomplishment to get this far). Have fun."

A black father who works for the school system has a friendly teacher show him his bright daughter's "confidential" record. In it is a five-page critique of how his own community activities as a "black militant" are causing his daughter to be "too challenging" in class.

Yet New York State has the clearest regulations in the nation concerning student records, thanks to a series of administrative and legal decisions dating back to 1960. In that year, the Levittown board of education directed that parents be permitted access to all the school records of their children, including evaluations, guidance notes and medical, psychiatric and psychological reports. A dissenting board member appealed the decision to the New York State commissioner of education. The result was a landmark ruling, *Matter of Thibadeau*, which specified that as a matter of law, parents have access to all their children's school records.

Yet in the following year, the administration in a neighboring New York school district refused to allow either the father or the private physician treating the former's son to see the boy's records. The father went to court, and the decision, *Van Allen* v. *McCleary*, stated: "It needs no further citation of authority to recognize the obvious 'interest' which a parent has in the school records of his Child." The court added that the parent's right to see the records stems from "his relationship with the school authorities as a parent who under compulsory education has delegated to them the educational authority over his child." Since both the Thibadeau and Van Allen rulings affected all New York State school systems, they became the basis for the detailed *Manual on Pupil Records* distributed to all school personnel.

Handed that clear mandate to allow parents access to records, how did the New York City school system respond? In May 1962, the board of education sent a special circular to all schools stating that most data in records—guidance notes, medical and psychological reports, social agency reports—"are not part of the official school record and are, therefore, not to be made available for parents to inspect." The system restated that policy in 1964 and 1969, insisting it was "in comformity with State regulations."

In 1970, the New York City system, disturbed by the publicity surrounding the Russell Sage guidelines and fearful of law suits, took a small step forward for privacy. It appointed an impressive committee of school department and civic representatives to review and help shape its policies.

An incident during the policy revision process said a good deal about the power of bureaucrats to ignore or override policy. The committee, hearing that school employees were regularly providing sensitive information about students to outside agencies, urged the chancellor to order an end to this practice until a new policy was settled on. He did so. Fifteen days later, under pressure from school administrators, he rescinded the order. During that short period of time, 28 separate and distinct categories of outsiders had called the board of education to complain that their usual sources of information about students had been cut off. They included FBI agents, military intelligence officers, welfare workers, policemen, probation officers. Selective Service board representatives, district attorneys, health department workers and civil service commission offices.

Inside education's own house, the most vocal opponents to giving parents access to student records are those who write and maintain the most sensitive and inferential records: the guidance counselors. In 1961, the American Personnel and Guidance Association issued a policy statement on the use of records that asserted that counselors have the right to decide which records parents should see and how those records should be interpreted to parents. The counselors generally argue this way: What if the child reveals a conflict with his parents that would only be aggravated if the parents knew what the child had said? What if a child tells of a home situation that may be defamatory or even illegal but is important to record for the future counseling of the student? What if parents misinterpret the professional notations of counselors? What if the child needs someone outside his home to confide in?

The other side of that argument is that if information is so delicate or painful that parents shouldn't see it, it probably shouldn't be in a school folder at all. Counselors answer that student evaluations will be badly watered down if those writing them know parents will see them—a statement that raises provocative

questions about the school's views of the parents of their students, and its honestry in dealing with them.

Dealing with this issue, the *Buffalo Law Review* pointed out in 1970 that when a school evaluates a child, it is acting *in loco parentis*, because evaluation is a parental function that has been extended to the school. But "once the school authority insists on keeping its evalaution of a child *secret*, then it introduces into the domain of parental prerogatives and oversteps its legitimate *in loco parentis* authority, for it is obvious that a parent can control publication of his evaluation of his own child and can keep secret from the world at large such evaluation."

There are, of course, circumstances in which the best interests of a child and inspection of his records by his parents may conflict. However, definition of those circumstances is made difficult by an unresolved ambivalence about whom counselors and school psychologists serve. If the counselor's client is the student, then the counselor should guard the pupil's records and interests zealously against all other parties, including other school employees. But if his client is the school system that pays him, and his job is trying to help adjust that student to the existing educational environment, then the counselor or psychologist might feel free to share personal information about the student with other educators and government agencies but not with parents, who become a sort of third party. Counselors who are used by school systems primarily to discipline truants and misbehavers unavoidably feel that the institution, not the child, is the client. Administrators all too often evaluate counselors not on the well-being of the child but on the thickness and currency of his record folder.

Perhaps the biggest problem faced by all concerned is the fact that we live today in a world of technologically recorded, maintained and communicated information. In 1968, the Phoenix, Arizona, Union High School System introduced a cumulative record system that enabled any staff member to pick up any phone in his school, push a button, dial a code number, dictate comments about a student into a remote recorder and play back comments made by other staff members. The comments, recorded on magnetic tape or a plastic disc in a central records room, are then transcribed by a typist onto pressure-sensitive labels that are entered in the student's permanent file. A clerk sorts the transcriptions, and they are delivered to the appropriate guidance counselor for inclusion in the cumulative record. Color coding identifies the kind of information contained on each gummed label—health, attendance, discipline or financial. Efficient, unquestionably. But what happens if a teacher calls in a comment at the end of a bad day and two weeks later regrets it, but the information has already made its way to the storage system? What if the typist misunderstands the dictation? What if the staffer dials a wrong number? The potential for abuse is staggering.

The state of Florida already has a centralized record-keeping computer system, which employs an IBM 1230 Optical Scanner to enter data for all pupils from the ninth grade on up into a computer. These items appear: Social Security number, grade, school, address, type of curriculum, date and place of birth, citizenship, health and physical disabilities, sex, race, religion, marital status, family background, languages spoken at home, academic record, test record, honors-work record and extracurricular activties. Iowa and Hawaii are installing similar systems.

Just last April the New York State Education Department asked 85 school districts to supply the names and addresses of all students who have received psychological or social work services; have a history of truancy, delinquency, drug abuse or alcoholism, or a "potentially disabling emotional, physical or mental handicap"; or have attended classes for unwed mothers, for the "socially maladjusted," or in drug-abuse prevention. In no cases were parents asked for permission to release the information.

Many systems complied. In one that didn't, Commack, New York, the director of pupil personnel services said his district would not send the names along "until I receive a statement . . . that they will not be put in a computer. . . ." The Nassau (County) Psychological Association took a strong stand against the information release, telling all schools: "Releasing this information without securing authorization from the parent or guardian is inimical to the professional behavior of the psychologist."

Even the federal government, not the greatest defender of privacy rights in recent times, has begun to show some concern about the possible adverse effects of computerizing personal records. An HEW task force on data banks, concerned

at first primarily with the recent push to require Social Security numbers of all children entering schools, has broadened its inquiry to include a wide range of other record problems. Another HEW group has been studying how records contribute to the systematic classifying and inappropriate labeling of school-children.

What is often described as California's "pioneering" work in social control suggests ways in which schools inadvertently may feed information about their students into Big Brother computers. With funds from Title I of the Omnibus Crime Control and Safe Streets Act of 1968, the California Council on Criminal Justice has set forth on the mission of making "Californians safe from crime." CCCJ funds a statewide program called "Correctionetics." It computerizes and centralizes all juvenile records, including information on psychiatric treatment. Under state law, children down to the age of six years who have been identified as being "in danger of becoming delinquent" can be declared "pre-delinquent" and thus become a California Youth Authority statistic with a juvenile record.

As if that weren't enough, CCCJ is looking for other potential problems that might be computerized. One program, funded for two years, instructed kindergarten teachers in sophisticated methods of identifying "target students"—those five-year-olds whose social and academic profiles were similar to those of adolescents who ended up in juvenile courts.

Suddenly, an unwary kindergarten teacher has become, in effect, a government intelligence agent.

Mr. Speaker, I think, upon a careful reading of this article, that one can more easily ascertain why this matter is of intense interest to myself and my colleagues.

The extent of information stored and used, and the potential abuses which arise therefrom, simply must be addressed by this and State legislative bodies.

I am committed to that task.

[From the Congressional Record, Extensions of Remarks, Apr. 5, 1974]

STUDENT RECORDS: A PROPOSED STRATEGY FOR PREVENTING ABUSES OF THE RIGHT TO PRIVACY

Mr. KEMP. Mr. Speaker, at this point in the proceedings, I include the second part of the research paper, entitled, "Students, Parents and the School Record Prison: A Legal Strategy for Preventing Abuses," by Sarah C. Carey, attorney at law:

[The paper follows:]

STUDENTS, PARENTS AND THE SCHOOL RECORD PRISON: A LEGAL STRATEGY FOR PREVENTING ABUSES—II

(By Sarah C. Carey)

A similar situation prevails in regard to State statutes governing access to the files. Most states do not guarantee parental access. At the same time, they leave the question of outside agency access up to the schools. For example, New Jersey in a fairly typical statute provides that "Public inspection of pupil records may be permitted and any other information relating to the pupils or former pupils of any school district may be furnished in accordance with rules prescribed by the state board and no liability shall attach to any member, officer or employee of any board of education permitting or furnishing the same accordingly." N.J. Stat. Ann. § 18A.36-19 (1939, 1968) No special mention is made of parents.

California, on the other hand, specifically grants a parent the right to inspect written records concerning his child "in any reasonable manner in consultation with a certificated employee of the district when he requests to do so during regular hours of the school day" Calif. Code Ann. Div. 9 Ch. 1 Art 6 § 10757 (Supp. 1973). The California statutes limit access to student records generally but spell out specific exceptions; these include a state or local law enforcement officer "seeking information in the course of his duties" or a county agency responsible for protective services to children. Limited exceptions are made for employers and for officials of the U.S. when the student is a veteran. § Calif. Code Ann. Div. 9, Ch. 1, Art. 9.

Oregon and Nebraska are unique in imposing stringent access provisions. Oregon makes student records confidential, grants the parents a broad right of

review of all records and limits access by others to grade transcripts, lists of courses taken, attendance records, achievement tests and health records. Ore Rev. Stat. § 336.19 (Supp. 1972) Nebraska's laws grant pupils and parents full access to their own records; deny access or divulgence of record contents to other persons; require that disciplinary files be maintained separately from performance records and mandate the destruction of the former after the student has graduated or left the school 3 poena) and 14 granted complete or partial access to prospective employers.[13]

Actual practice even in those states with express statutory provisions tends to favor access by public officials, while disfavoring the parent.[14] The Russell Sage Survey,[15] published in 1969 reported that of the 54 school districts examined, 20 districts denied access to the entire file to parents; 14 denied access to part of the file and 8 allowed access under certain circumstances only. On the other hand, 29 districts granted full access to CIA and FBI officials, 23 granted such access to the juvenile courts (without a subpoena) and 14 granted complete or partial access to prospective employers.[16]

C. *The legal rights of the parent:* The United States Constitution guarantees to the Individual citizen a series of fundamental rights that cannot be infringed by the federal or state governments without compelling justification. Current definitions of these rights include the right to marry,[17] the right to bear children, and maintain a family,[18] the right to control one's body,[19] and the right to direct the upbringing of one's children.[20] The essence of these rights is that they are so fundamental to personal liberty that they merit a high level of protection from incursions by the state. They are sometimes described as "fundamental" or "natural rights" inherent in American tradition or Western values; in other cases they are posited upon the 14th Amendment's guarantee of liberty or the 9th Amendment's reservation of rights to the people; and in still others they are based on common law principles.

Whatever the basis, it is clear that a parent, as part of his right to raise a family, retains basic decision-making authority and responsibility concerning his child's education that cannot be abridged by the states whether by direct exclusion of the parent or by indirect exclusion through the withholding of crucial information about the child.

(1) *The Parent Can Control Certain Basic Aspects of His Child's Education.* (a) *The "Due Process" Decisions*: In a series of major decisions, the U.S. Supreme Court has ruled that the guarantee of liberty contained in the 14th Amendment due process clause insures the right of the parent to control the upbringing of his children. That clause provides that no state may "deprive any person of life, liberty, or property, without due process of law." The precision content of the concept of "liberty" protected under this provision has been the subject of extensive debate, but it has generally been understood to encompass both those rights explicitly enumerated in the Bill of Rights as well as additional rights traditional to this society.[21]

The first decision by the U.S. Supreme Court reserving basic control over a student's education to his parents was *Meyer* v. *Nebraska* 262 U.S. 390 (1923). In that case the Court declared unconstitutional a state law that prohibited the teaching of "any subject to any person in any language other than the English language." The statute also forbade the teaching of foreign languages until the pupil had successfully passed the eighth grade. The Court held that such legislation could not be justified under the guise of protecting the public; on the contrary it took judicial notice of the fact that "experience shows that this (instruction in a foreign language at an early age) is not injurious to the health, morals, or understanding of the ordinary child." It concluded instead that the statute was an unwarranted interference "with the opportunities of pupils to acquire knowledge, and with the power of the parents to control the education of their own." [22]

The Court found that the latter was an integral part of the liberty guaranteed by the due process clause. It stated:

"Without doubt, it (liberty) denotes not merely freedom from bodily restraint, but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free man." 262 U.S. at 399.

In 1925, in *Society of the Sisters of the Holy Name of Jesus and Mary* v. *Pierce*, 268 U.S. 510 (1925), the Court further elaborated on the control of the

Footnotes at end of article.

parent over the child's education. There, the Court invalidated an Oregon compulsory education law requiring the attendance of all students at public schools. Parents who wanted to send their children to parochial schools[23] had claimed that the law interfered with their right to religious freedom and to the upbringing of their children. In an opinion that put little emphasis on the First Amendment allegations the Court held:

"Under the doctrine of *Meyer* v. *Nebraska* . . ., we think it entirely plain that the Act of 1922 unreasonably interferes with the liberty of parents and guardians to direct the upbringing and education of children under their control. As often heretofore pointed out, rights guaranteed by the Constitution may not be abridged by legislation which has no reasonable relation to some purpose within the competency of the state. The fundamental theory of liberty upon which all governments in this Union repose excludes any general power of the state to standardize its children by forcing them to accept instruction from public teachers only. The child is not the mere creature of the State; those who nuture him and direct his destiny have the right, coupled with the high duty, to recognize and prepare him for additional obligations." 268 U.S. at 534–35.

In subsequent years the Court repeatedly acknowledged the sanctity of the family relationship, and the right and duty of the parent to provide for the education and upbringing of his children.[24] In 1972, in *Wisconsin* v. *Yoder*, 406 U.S. 205, the Court excused Amish children of senior high school age from compulsory school attendance altogether, finding that the society in which they lived imparted to them a different but equally valid set of values and skills. Although there were religious overtones to the case, the Court held that the parents could choose the education scheme that best met the principles underlying their way of life, provided the latter was sufficiently defined. The Court rejected the state's argument that it was acting as *parens patriae*, suggesting that the state could assert that role over the parent's interest only if there were a showing of harm to the physical or mental health of the child or to the public safety, peace, order or welfare.

In reaching its decision to excuse Amish children from the state's compulsory education requirement, the Court reasoned as follows:

"The history and culture of Western civilization reflect a strong tradition of parental concern for the nurture and upbringing of their children. This primary role of the parents in the upbringing of their children is now established beyond debate as an enduring American tradition. . . . To be sure, the power of the parent, even when linked to a free exercise claim, may be subject to limitation under *Prince* if it appears that parental decisions will jeopardize the health or safety of the child, or have a potential for significant social burdens.

* * * * * * *

"(A) State's interest in universal education, however highly we rank it, is not totally free from a balancing process when it impinges on other fundamental rights and interests, such as those specifically protected by the Free Exercise Clause of the First Amendment and the traditional interest of parents with respect to the religious upbringing of their children . . ." 406 U.S. at 232, 233, 234, 214.

The Supreme Court decisions do not cover a broad variety of factual circumstances. And they have made it clear that the rights of the individual parent were preserved because there was no serious conflict with countervailing state interests, such as protection of the public health or safety. Despite their limited reach,[25] it can be argued on the basis of these cases that the parent has a right to make affirmative decisions concerning his child's disposition; particularly where spiritual, cultural, or psychological factors are involved. As stated above, the Court has not yet had to deal with the question of whether the parent also has a right to any records maintained by the school that are necessary to the proper exercise of his decision-making authority. However, such access should be viewed as an integral part of the basic parental right. It is unlikely that the Court would define a fundamental right on the one hand and then permit the schools to frustrate it by denying the means essential to its exercise on the other.[26]

(b) *The Ninth Amendment:* A second, to some extent overlapping, constitutional source of protecting a parent's right to control his child's education can be found in the Ninth Amendment to the U.S. Constitution. That amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." The Court has

Footnotes at end of article.

rarely elaborated upon this amendment; in fact, it was not raised with any frequency until the advent of the privacy cases; it has received further elaboration in cases challenging abortion laws;[27] laws that interfere with personal appearance and similar interferences with the person.[28]

The most extensive discussion of the reach of the Ninth Amendment is contained in Justice Goldberg's concurring opinion in *Griswold* v. *Connecticut*, 381 U.S. 479, 486 (1965). Goldberg, in arguing that the right to privacy in marriage (and hence to choose to use or not use contraceptives), although not mentioned in other sections of the Constitution, was a right contemplated by the 9th Amendment, stated:

"The 9th Amendment simply shows the intent of the Constitution's authors that fundamental rights exist that are not expressly enumerated in the first eight Amendments and an intent that the list of rights included there not be deemed exhaustive." 381 U.S. at 492.

Goldberg argued that the rights additional to the enumerated ones could be determined by looking: "to the 'traditions and (collective) conscience of our people to determine whether a principle is so rooted (there) . . . as to be ranked as fundamental.' . . . The inquiry is whether a right involved 'is of such a character that it cannot be denied without violating those fundamental principles of liberty and justice which lie at the base of all our civil and political institutions'. . . . '. . . 'Liberty' and 'gains content from the emanations of . . . specific (constitutional guarantees) and 'from experience with the requirements of a free society.'" 381 U.S. at 493.

This language suggests that in many, but not necessarily all cases, considerable overlap will exist in the definitions of: 9th Amendment rights, the rights encompassed within the liberty promised by the due process clause, and the common law rights accruing to the individual vis-a-vis the state. In any challenge asserting a parental right to control his child's education all three sources of authority should be relied upon.[29]

FOOTNOTES

[13] Massachusetts recently enacted a parental access law that states: "Each school committee shall, at the request of a parent or guardian of a pupil or at the request of a pupil 18 years of age or older allow such parent, guardian or pupil to inspect academic, scholastic or any other records concerning such pupil which are kept or required to be kept." Ch. 785 Acts of 1973 General Laws Ch. 71, Sec. 34 E.

[14] Diane Divoky "Cumulative Records: Assault on Privacy", Learning Magazine.

[15] Footnote 3, p. 6 *supra*.

[16] A recent article on New York City showed that 28 "outside agencies had access to the school records". These included FBI agents, military intelligence officers, welfare workers, policemen, probation officers, Selective Service board representatives, district attorneys, health department workers and civil service commission officers.

[17] *Loving* v. *Virginia*, 388 U.S. 1 (1967).

[18] *Skinner* v. *Oklahoma*, 316 U.S. 535 (1942); *Meyer* v. *Nebraska*, 262 U.S. 390 (1925).

[19] *Roe* v. *Wade*—U.S.—35 L.Ed. 2d 147 (1973); *Stull* v. *School Board of the Western Beaver Junior-Senior High School et al.* 459 F.2d 339 (1972).

[20] *Wisconsin* v. *Yoder*, 406 U.S. 205 (1972); *Meyer* v. *Nebraska*, 262 U.S. 390 (1923); *Society of the Sisters of the Holy Name of Jesus and Mary* v. *Pierce*, 268 U.S. 510 (1925).

[21] These rights cannot be interfered with without substantial justification. In the words of Justice Douglas:

"Due process has not been reduced to any formula; its content cannot be determined by reference to any code. The best that can be said is that through the course of this Court's decisions it has represented the balance which our Nation, built upon postulates of respect for the liberty of the individual, has struck between that liberty and the demands of organized society. . . . It is a rational continuum which, broadly speaking, includes a freedom from all substantial arbitrary impositions and purposeless restraints" (*Poe* v. *Ullman*, 367 U.S. 497 (1961) dissenting opinion.)

[22] The court also suggested that the state could not err in the other direction by overreaching in its educational offerings. It took the example of Sparta where "in order to submerge the individual and develop ideal citizens," the males were assembled at seven "into barracks and entrusted their subsequent education and training to official guardians." The Court commented that although such measures "have been deliberately approved by men of great genius, their ideas touching upon the people of a state were wholly different from those upon which our institutions rest; and it hardly will be affirmed that any legislature could impose such restrictions upon the people of a state without doing violence to both letter and spirit of the Constitution."

[23] The Court also found an unjustified interference with the property rights of the private church schools.

[24] In *Prince* v. *Massachusetts*, 321 U.S. 158 (1943), for example, the Court upheld a statute prohibiting the sale or offer of sale of periodicals, magazines or other literature, including religious literature, on the streets or in other public places by minors but stated that "It is cardinal with us that the custody, care and nurture of the child resides first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder. . . . And it is in recognition of this that these decisions have respected the private realm of family life which the state cannot enter." Similarly in *Griswold* v. *Connecticut*, 381 U.S. 479 (1965) striking down a Connecticut law that proscribed the use of contraceptives by married people, the Court referred to the right of a parent to control his child's education established in *Pierce* and *Meyer*, as a precedent for deriving marital privacy rights from the 1st and 14th Amendments.

[25] One lower federal court has applied the right of parental control contemplated by the due process clause to preclude the exercise of corporal punishment by the school against the child. In *Glaser* v. *Marietta*, 351 F. Supp. 555 (W.D.Pa 1972) the Court stated: "The regulations enacted by the School District on their face appear to be reasonable, within the scope of authority which the state is authorized to grant to it, and in agreement with the preference of many parents. But when the regulations are confronted with the flat prohibition of a particular parent and an assertion of her fundamental rights to raise her child in the manner in which she chooses, then obviously the balancing process inherent in the *Yoder* and *Prince* cases becomes necessary." 351 F. Supp. at 560. The Court acknowledged that judicial interference with school decisions was not advisable unless basic rights were involved; it then held that the judgment as to the appropriate form of punishment for a wayward student "is that of the parent primarily, not the state, not the school and may be made by the parent absent weighty factors which we do not find exist in this case. Where justification for the deprivation of a personal liberty cannot be shown, it may not be taken away by the state or its agency." 351 F. Supp. at 561. The Court added that any parent who was unwilling to grant punishment discretion to the school had an obligation to discipline the child herself so that he would not interfere with other children. (Some federal courts have reached divergent results in regard to discipline issues).

[26] In addition to the federal court decisions basing a parent's right to determine the education of his child on the 14th Amendment's due process clause, a number of state courts have reached similar results. See, for example, *Finot* v. *Pasadena City Bd. of Ed.*, 58 Cal. Rptr. 520; 250 C.A. 2d 226 (1967) and *Dickens* v. *Ernesto*, 37 A.D. 2d 102, 322 N.Y.S. 2d 581 (1971).

[27] YWCA of *Princeton* v. *Kugler, et al.*, 342 F. Supp. 1048 at 106 (D.N.J. 1972), *Roe* v. *Wade*, 410 U.S. 43, 35 L. Ed. 2d 147 (1973).

[28] See, for example, *Breen* v. *Kahl*, 419 F. 2d 1034 (1969) and *Stul* v. *School Board of Western Beaver Junior-Senior High School et al.*, 459 F. 2d 339 (1972) upholding a right to determine one's own hair style. The *Breen* Court held this to be an aspect of personal freedom whether designated "as within the pneumbras of the First Amendment freedom of speech . . . or as encompassed within the Ninth Amendment as an additional fundamental right." 419 F. 2d at 1036.

[29] Some states have included in their own constitutions clauses similar to the 9th Amendment. Article 1 section 31 of the Idaho constitution, for example, states: "This enumeration of rights shall not be construed to impair or deny other rights retained by the people." In 1957, the Supreme Court of Idaho in *Electors of Big Butte Area* v. *State Board of Education*, 78 Idaho 602; 308 P.2d 225 (1957), held that among these rights is the right of parents to participate in the supervision and control of the education of their children.

[From the Congressional Record, Extensions of Remarks, Apr. 9, 1974]

Student Records: A Proposed Strategy for Preventing Abuses of the Right to P'...acy

Mr. Kemp. Mr. Speaker, at this point in the proceedings, I include the concluding part of the research paper, "Students, Parents, and the School Record Prison: A Legal Strategy for Preventing Abuses," by Sarah C. Carey, attorney at law:

[The paper follows:]

Students, Parents, and the School Record Prison: A Legal Strategy for Preventing Abuses—IV

(By Sarah C. Carey)

Due process requirements [42] have recently been extended by the Courts beyond expulsion situations to situations involving exclusion from the school system altogether or denial of mainstream educational opportunities because of assignment to special classes.[43] In *PARC* v. *Pennsylvania*, 334 F. Supp. 1257 (E.D.P. 1971) procedural guarantees were imposed through a consent decree on the Pennsylvania school system in regard to decisions to exclude mentally retarded students from the school system or to shift them among various alternative institutions in an arbitrary manner. And in *Mills* v. *Board of Education of D.C.* 348 F. Supp. 866 (1972), the district court for the District of Columbia imposed similar requirements on school authorities assigning handicapped children and those with special learning problems to special programs. The Court held that regular public school assignments or "equal" education was an entitlement of the children that could not be denied or restricted without a full hearing. The Court outlined the procedures required to protect parental rights as follows:

"Before placing a member of the class in such a program, defendants shall notify his parent or guardian of the proposed educational placement, the reasons therefore, and the right to a hearing before a Hearing Officer if there is an objection to the placement proposed."

The Court also specified that the notice to the parents must "clearly state the specific and complete reasons for the proposed action, including the specifica-

---

Footnotes at end of article.

tion of any tests or reports upon which such action is premised." Further, the notice must inform the parents of the right "*to examine the child's school records before the hearing, including any tests or reports upon which the proposed action may be based.*" (emphasis supplied) The Court indicated that the right to examination extends to all public records bearing on the decision about the child."

These decisions represent substantial judicial incursions into areas previously reserved to teachers, counsellors and school administrators. They make it clear that the power exercised by the schools in regard to students is too great and the consequences that flow from adverse decisions in regard to the individual are too significant to permit the schools to act in an arbitrary or unfair fashion. The law requires that where a decision by school authorities does not involve a minor ministerial or disciplinary matter but represents a major change in the opportunities afforded the student that carries with it the potential of real injury, the Courts will require a fair hearing for the child and an opportunity for him to present his own case. This means, as a practical matter, that any important decision with potentially injurious consequences cannot be taken without disclosure of the records, assessments and other data upon which it is based. And if the underlying data or assessments are found to be invalid, the decision of the school officials will be reversed (See, for example, *Larry P.* v. *Riles*, supra p. 2, where an assignment of certain Black students to classes for the educable mentally retarded was reversed because it was based primarily on IQ tests that were found to be racially discriminatory).

What remains unclear is the precise delineation of the kinds of adversary rights assured to the student and the range of situations to which they will apply. This will evolve as different factual situations are presented to the Courts. At a minimum, where the decision is an important one, the student is guaranteed the right to notice as to the specific charges against him, the right to learn the evidence upon which the school's determinations were based and the right to present his own case.

In at least one case, *Medera* v. *Board of Education of the City of New York* the question of the student's right to have his attorney participate in a school hearing that could result in his suspension from school was addressed. Although the trial Court upheld the student's right to counsel thereby invalidating a school regulation to the contrary (267 F. Supp. 356 S.D.N.Y. 1967),[45] the Court of appeals reversed the decision, on the grounds that the hearing was preliminary in nature and was designed to plan for the child's educational future, rather than to punish him. (386 F. 2d 778 2nd Cir. 1967; cert, denied 390 U.S. 1029 1968). The appellate ruling bent over backwards to minimize the injurious consequences flowing from the hearing, equating assignment to a school for socially maladjusted children with poor grades or an order to repeat a grade, and characterizing the school as being on the side of the child rather than his adversary, as appeared to be the case.

Most school proceedings that threaten invasions of a child's rights probably do not require the formality of legal counsel, provided the parents and the child are capable of presenting their case. However, in areas where medical or psychological grounds, unintelligible to the layman, are given for a particular decision, the parent should be permitted to consult and present his own expert witnesses.[46]

(4) *The Parent Has a Right to Challenge Inclusion of Certain Information in His Child's File as Well as Its Distribution to Non-School Personnel:* In addition to wanting to gain access to the information that the school has placed in his child's file, a parent may want to restrict the collection of certain kinds of information altogether and/or to prevent its distribution to non-school personnel.

(a) *The right to Privacy:* Some of the data currently maintained in children's files, particularly anecdotal information about his family or psychological assessments of his background could probably be challenged as invading the child's or the parents right to privacy. This right, as defined in the Supreme Court's decisions in regard to abortion, contraceptives and other matters, is inherent in the first nine amendments to the US Constitution. These amendments guarantee privacy in regard to those personal rights that are deemed fundamental or "implicit in the concept of ordered liberty". As stated in *Roe* v. *Wade* 410 U.S. 43 (1973), this encompasses:

"Activities relating to marriage, *Loving* v. *Virginia* 388 U.S. 1,12 (1967), procreation, *Skinner, Oklahoma*, 316 US 535, 541–542 (1942) contraception, *Eisenstadt* v. *Baird*, 405 US at 435–454 ic. at 460, 463, 465 (White J. Concurring

Footnotes at end of article.

in result); family relationships, *Prince* v. *Massachusetts*, 321 US 158, 166 (1944) and child rearing and education, *Pierce* v. *Society of Sisters*, 268 US 510, 535 (1925), *Meyer* v. *Nebraska*, *supra*." (at 152–153)

Under these principles, the schools should not be allowed to collect data on students that intrude upon family relationships or the right of the parent to rear his child. At least one federal court has applied this standard to a situation where a public school, as part of a drug prevention program, attempted to collect highly intimate details on the relationship of the child to his parents and of the parents to each other.[47] In *Merriken* v. *Cressman*, supra p. 4 the Court reviewed the questionnaire given to each student and concluded:

"These questions go directly to an individual's family relationship and his rearing. There probably is no more private a relationship, except marriage, which the Constitution safeguards than that between parent and child. The Court look upon any invasion of that relationship as a direct violation of one's Constitutional right to privacy.

The Court stated that the school had provided insufficient justification for its program and, in addition, had failed to obtain an "informed consent" from the parents involved. So holding ,the Court ordered the termination of the program.

(b) *The Right to Procedural Due Process to Prevent "Stigma":* Other data such as assessments of learning disabilities that involve medical or other labels suggesting inadequacy or inferiority can be excluded on the grounds that they stigmatize the child without affording him due process. In addition to the right to challenge exclusionary and other prejudicial decisions flowing from such assessments (see Sec. 3 supra), a parent has the right to exclude the assessment or underlying data itself from his child's file to prevent reliance upon its for other purposes.

A series of Supreme Court decisions have established that the state cannot give an individual a prejorative label that will interfere with his right to life and liberty without guaranteeing him procedural due process. For example, in *Joint Anti-Fascist Refugee Committee* v. *McGrath*, 341 U.S. 123 (1951) the Supreme Court held that the Attorney General could not stigmatize a person by placing him on his subversive list without giving that person a right to be heard.

In the more recent case of *Wisconsin* v. *Constantineau*, 400 U.S. 433 (1971) the Court struck down a Wisconsin law that permitted the police chief to label an individual an habitual drunkard and to so notify local liquor stores, forbidding them to sell her liquor. The Court did not question the state's right to protect itself against public drunkenness; it concluded instead that such a label is a "badge of infamy" that the state may not attach without first providing an opportunity for challenge. "When a person's good name, reputation, honor or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential". (at 437). The Court emphasized procedural fairness as a necessary check on government power.[48]

Even in regard to records of the criminal justice system, an area where the State has extraordinary powers in regard to the citizen, the Courts have intervened where false or erroneous arrest records have been disseminated about an individual. * * * In *United States* v. *Kalish*, 271 F. Supp. 968 (D.P.R. 1967), for example, the Court held that an individual who had been erroneously arrested was entitled to have his photographs and fingerprints taken at the time of arrest expunged. The Court noted that maintenance of such records served no "public good" and stated that:

"His privacy and personal dignity is invaded as long as the Justice Department retains 'criminal' identification records, 'criminal' arrest, fingerprints, and a rogues' gallery of photographs." 271 F. Supp. at 970.

The *Cressman* Court, *supra*, based part of its decision on a finding that the assessment tools for determining which children might be potential drug users were too unreliable considering the seriousness of the label that would be imposed on the child. The Court stated:

"The ultimate use of this information . . . is the most serious problem that faces the Court. How many children would be labeled as potential drug abusers who in actuality are not? . . . When a program talks about labelling someone as a particular type and such a label could remain with him for the remainder of his life, the margin of error must be almost nil."

The Court pointed out that outside authorities including the district attorney, hospitals, rehabilitation personnel and others could obtain the information

---

Footnotes at end of article.

suggesting that a particular student was a drug problem and would treat him accordingly.

Similarly, the federal district court for the Northern District of California, found in *Larry P.* v. *Riles*, 343 F. Supp. 1306 (N.D. Calif. 1972), that a child would be unlawfully labeled by including in his permanent record the results of a racially discriminatory IQ test and a subsequent classification as "educable mentally rearded"; the Court noted that the harmful effects to the child would extend; to the Armed Services, employers and others with access to the file.[49]

Taken together, the "stigma" and the privacy cases suggest that in school districts where data that imposes a negative label of dubious validity on the child, or data of a highly personal nature are included in the child's file, the parent can seek not only to have the material removed from the file but to bar its collection in the first place.

CONCLUSION

The constitutional and case law principles discussed throughout this article have been raised in a variety of factual and legal contexts. Although many of the situations arising today where parents are concerned that school authorities have interfered with their prerogatives are factually more complex than the situations involved in earlier common law and constitutional decisions, the principles articulated in those cases continue to be valid today. Properly developed and applied, they can be relied upon to correct situations where the schools have exceeded the authority delegated to them by the parent. A key area for such application is the retention by the schools of personal, subjective or unverifiable assessments and records on a student and the withholding of such records from those most concerned—the parent and the child.

FOOTNOTES

[42] In addition to insisting on procedural due process prior to expulsion from schools, a number of decisions have voided school board regulations that by their own terms, exclude certain kinds of children. In *Ordway* v. *Hargraves*, 323 F. Supp. 1155 (D. Mass. 1971), for example, the Court declared unconstitutional a rule excluding pregnant students from the school where there was no showing that the plaintiff interfered with the education of other children or in any way endangered her own health. In *Hosier* v. *Evans*, 314 F. Supp. 316 D. St. Croix 1970) the Court voided a school regulation that excluded alien children from the public schools in situations where there was overcrowding.

[43] This principle is similarly reflected in recent cases holding that the parent cannot waive his right to meaningful participation in decisions concerning his child or consent to potentially detrimental treatment by the school by his child unless his consent or waiver is an informed one. *Larry P.* v. *Riles* supra p. 5; *Merriken* v. *Cressman*, supra p. 7. (See also *Madera* v. *Board of Education of the City of New York*, 267 F. Supp. 356, at 372 (S.D.N.Y. 1967) at p. 372).

[44] The *Mills* decision cited as precedent *Goldberg* v. *Kelly*, 397 U.S. 254 (1969), a case guaranteeing welfare recipients the right to a hearing prior to the termination of benefits. In that case the Supreme Court held that due process principles require "that a recipient have timely and adequate notice detailing the reasons for a proposed termination, and an effective opportunity to defend by confronting any adverse witnesses and by presenting his own arguments and evidence orally." The welfare decisions, and the administrative regulations issued to insure conformity with them as well as similar decisions dealing with terminations of unemployment insurance, public housing ets. . . . shed additional light on the nature of the procedures that are required to meet due process standards. See also *Hobson* v. *Hansen*, 269 F. Supp. 401 D.D.C. (1967); *Smuck* v. *Hansen*, 408 F. 2d 175 (D.C. Cir. 1969); *Hobson* v. *Hansen*, 327 F. Supp. 844 (D.D.C. 1971), for the rights of a parent in regard to a decision by the public school system to "track" his child.

[45] The lower court decision includes an illuminating account of the broad distribution of student records in the NYC school system, and of the punitive role often played by psychologists and social workers in an allegedly therapeutic context.

[46] For a further elaboration of the need for this approach see Kirp, David L. "Schools as Sorters: The Constitutional and Policy Implications of student classification." Vol. 121, No. 4, Univ. of Pa. L.R. 705, at 789 (April, 1973).

[47] The questionnaire included such items as the religion of the student, the family composition, including the reason for the absence of one or both parents and whether one or both parents "hugged and kissed me goodnight when I was small," "tell me how much they love me," "enjoyed talking about current events with me," and "make me feel unloved."

[48] See also *Board of Regents* v. *Roth*, 408 U.S. 564 (1972) a case brought by a non-tenured faculty member challenging his dismissal because he was not granted a hearing. The Court held that simple dismissal was not enough to stigmatize but suggested that if the State had charged him with behavior that might "seriously damage his standing and associations in his community" he would be entitled to a hearing. * * * In a decision restricting the dissemination of arrest records for non-criminal justice purposes, the court in *Menard* v. *Mitchell*, 328 F. Supp. 718 (D.D.C. 1971) noted: "Systematic recordation and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move about in this land." 328 F. Supp. at 726.

[49] Where the classification or label assigned to a child is likely to have profound consequences on employment opportunities, the reasoning of the Supreme Court in *Greene* v. *McElroy*, 369 U.S. 474 (1959), a case where the Secretary of Defense had revoked a security clearance without affording confrontation and cross-examination, would seem to apply. There the Court stated: "Certain principles have remained relatively immutable in our jurisprudence. One of these is that where governmental action seriously injures an individual, and the reasonableness of the action depends on fact findings, the evidence . . . must be disclosed to the individual so that he has an opportunity to show that it is untrue . . . The Court has been zealous to protect these rights from erosion. It has spoken out not only in criminal cases . . . but also in all types of cases where administrative and regulatory actions were under scrutiny". 369 U.S. at 497–8.

A COMMITMENT

As a member of the Committee on Education and Labor—which has legislative jurisdiction over both the Elementary and Secondary Education and Higher Education Acts, as well as other related Federal statutes—I am deeply committed to the enactment of safeguards to protect parents' and students' rights to the privacy of information maintained in student records.

This is not wholly a Federal concern. Responsibility for education rests primarily—as it should—with the State and local governments. A legislative strategy will, therefore, have to necessarily involve the enactment of law at all levels—Federal, State, and local.

This matter is now under intense scrutiny by staff, and I hope to report to the House within the very near future on the courses of action most appropriate to be followed.

[From the Congressional Record (Pt. II), Extensions of Remarks, Apr. 11, 1974]

AMONG THE POTENTIAL PROBLEMS ASSOCIATED WITH SENSITIVITY TRAINING

Mr. KEMP. Mr. Speaker, Prof. James Likoudis, of Williamsville, in an article he wrote for the Social Justice Review, begins his article by quoting a very thoughtful and cogent editorial published in our Buffalo, N.Y., Catholic Diocesan newspaper, with which I fully concur. The editorial said in part:

"For centuries, the family unit has been regarded as the transmitter of cultural heritage, and respect for the dignity and authority of parents. However, in the past 50 years, attempts have been and are being made to erode these principles and the privacy of the family structure, particularly by many modern educators, psychologists and sociologists."

Mr. Speaker, Skinnerian philosophy manifested in sensitivity training and other behavioral modification techniques poses a real threat to the sanctity of the family unit and to the cherished right to privacy.

There has been much discussion over the past several years on the advisability of using so-called sensitivity training. As a member of the House Committee on Education and Labor, I have read and heard much of the debate on this issue.

Unfortunately, too much of this debate has not been adequately based upon a full review of the facts and appreciation for the relevance of the hard facts used to formulate the positions which have been taken on this issue. This should not be the case any further, for in dealing with this issue we are dealing with the most vital and important aspects of human individuality.

I believe Professor Likoudis has made a significant contribution to the discussion on this issue, a contribution of singular clarity, one buttressed by extensive documentation and authority. It is entitled, "The Menace of Sensitivity Training: The Mind Manipulator," which appeared in the February 1973 issue of Social Justice Review.

Mr. Speaker, at this point in the Record, I include the text of the article:

[The article follows:]

THE MENACE OF SENSITIVITY TRAINING: THE MIND MANIPULATOR

(By James Likoudis)

On July 27, 1972 the Buffalo, N.Y., diocesan newspaper, The Magnificat, published a remarkable lead-editorial which was reprinted in other Catholic newspapers. It was entitled: Threat to Family Life and deserves quotation in full.

"For centuries, the family unit has been regarded as the transmitter of cultural heritage and respect for the dignity and authority of parents. However, in the

past 50 years, attempts have been and are being made to erode these principles and the privacy of the family structure, particularly by many modern educators, psychologists and sociologists.

"There exists a movement generated by the National Educational Association and others, to introduce behavior modificaton techniques in schools to 'improve patterns of behavior and help adjustment.' In the questionable name of education, these programs constitute an invasion of privacy, of the freedom from coercion, and of the rights of parents to raise their children in their own value-system and beliefs.

"In essence, these behavior and modification techniques range from Skinnerian operant conditioning, family life programs including sex education, role-playing, psychological tests, sensitivity-training techniques of sorts, group confrontation techniques and group criticism. They are all akin to brain-washing techniques designed to promote attitudinal changes with trained teachers acting as parent surrogates. The idea is to transform American schools into human relations training institutes with social scientists teachers and 'effective trainers.'

"This trend is dangerous and unconstitutional, fraught with totalitarian aspects. There have been many fads in psychology and the current, widespread embracing of group encounters is the latest. Known as marathon encounters, sensitivity training, T-groups, nude therapy, encounter groups, etc., these groups are small gatherings of people in which interpersonal confrontations are encouraged for the purpose of influencing attitudes and developing skills towards more productive social interactions. While it sounds admirable, these techniques are not universally applicable and can be highly disturbing emotionally to some individuals. There is a 10% casualty rate in encounter groups and this form of therapy is not an accepted form of treatment by the American Psychiatric Association.

"Other dangers are that these techniques do not take into consideration the personality of the child; that teachers are not capable of handling crises; that they produce short-term effects; that some students can't take exposure of faults nor criticism; that borderline psychotic cases can collapse; that these techniques represent an invasion of a child's private thoughts. It is mandatory that schools return to the basic function of education, a formidable task in light of the fact that deficiencies in writing, spelling grammar and reading are serious problems today. As someone aptly put it, we seem to be getting 'Woolworth education at Tifanny prices.'

"Sensitivity training techniques do not belong in the classroom as they lead to a totalitarian-style educational system with secrecy for the regime and constant surveillance of the students. Children need privacy as room to grow in, to explore the world within and without. They also need to identify with parental values, not those of educators whose morality and values may be different."

Yet another voice has been heard from within the councils of the U.S. Catholic bishops to question the morality of psychological techniques being utilized to alter human consciousness and awareness. At the Bishops' Conference in November 1972, Bishop Mark Hurley of Santa Rosa, California who heads a committee, the *Secretariat for Human Values*, spoke sharply concerning human values being increasingly denied by a "world that has become more and more secularized, depersonalized, and dehumanized."

"Is it not time," he said, "that some moral judgments be assessed on the experiments in the field of psychology? I refer specifically to sensitivity and encounter sessions. There is a growing list of scientific books and articles which are beginning to question, to make value judgments. Some research suggests that sensitivity training sessions have caused deleterious effects to mental health in as high as seven in ten cases in the studies made. Two other questions are being asked as well: Do these sessions really protect the privacy of persons who participate? Do these sessions not tend to the violation of natural secrets and indeed, sometimes, of committed secrets?" (*Wanderer* 11-30-72)

This concern expressed by a bishop would appear to be timely in view of the alarming impact of the "sensitivity cult" in the Church itself. Widespread introduction of Group Dynamics and sensitivity training techniques into all forms and levels of Catholic education is intimately linked to the apostasy of certain priests and religious, decimation of the religious orders, virtual displacement of authentic religious education by "relationship education" or "experimental catchesis," shocking proliferation of naturalistic sex education in Catholic schools, and spiritually barren "horizontalism" characterizing the attitudes of liberal Catholics. Even Fr. Andrew Greeley (who has not scrupled to declare publicly that the

American bishops were "intellectually, spiritually and morally bankrupt") has openly avowed:

"One wonders whether the current romance between American Catholicism and group dynamics can lead to anything but tragedy. The "sensitivity" cult is a marvellous symbol of the superficial, shallow, anti-intellectual romanticism which presently besets the American Church and which seems likely to cause religious impotence.

"Make no mistake about it. Substantial segments of the elite groups in American Catholicism are hooked on an extraordinary collection of group experiences running all the way from the quite limited 'orthodox' T-groups sponsored by the National Training Laboratories to the berserk nude marathon sessions of the Esalen variety. If one can explain the overwhelming popularity, not to say virtually unquestionable sanctity of groupism to many Catholics, despite the fact that the theories behind such group experiences are questionable, the practical results are dubious and dangers are evident, one will have gone a long way toward the present crisis in the American Catholic Church. . . .

"The dramatic change created in the Church by the Vactican Council has destroyed many outmoded structures but, in the process, we have become a church without theological or organizational context. Emphasis on process and relationship are an excuse from the hard, difficult task of developing new intellectual visions and new organizational structures. Indeed the church seems to have become one gigantic T-group with little structure, high levels of anxiety, and vast regressions to infantile behavior patterns." (National Catholic Reporter 5–1–70, pp. 10–11)

It is perhaps well to recall at this point that Sensitivity Training is also known under many other names: Group Dynamics, Therapy for Normals, Leadership Training, Group Confession, Interpersonal Competence, Marathon Labs, Confrontation Sessions, Interpersonal Relations, Human Relations Lab, Self-Evaluation, Human Potential Workshop. T-Group Training, Auto-Criticism, Operant Conditioning, Self-Honesty Sessions, Non-Verbal Exercises, Body Awareness, Syanon Games Clubs, Basic Encounter Group, etc. Whatever the name utilized, the goal of sensitivity training is clearly to strip from the individual those inhibitory attitudes, feelings and values which prevent adjustment to allegedly more open, free, honest and authentic group standards. Individual thinking is, in effect, displaced by group feeling.

If, as shall be noted, there is already sufficient evidence to question the morality of Sensitivity Training techniques in the case of adults, the gross application of such techniques in the education of children is even more reprehensible.

For years, acute critics of American education have warned that it is no longer liberal in the traditional sense. Education, they have stressed, is increasingly considered a means of social experimentation, cultural control, and political indoctrination—with schools taking on the form and function of psychosocial "clinics" demanding the *total control* of the child. A young Catholic political philosopher, Paul Cole Beach, has written with profound insight:

"These new school trends are clearly seen in a sex education calculated to change radically the traditional concepts of sexual morality and the family, and to replace them with the values of a contraceptive society. New trends in teaching methods are most dramatic yet, particularly the stress on psychiatric techniques and behavioral psychology. Group Therapy methods which change a person's attitudes and values are being woven into every level of public education—from teacher training to the classroom itself. Students are being subjected to psychiatric techniques which are calculated to substitute group opinion for the integrity of personal judgment. Public education is now meant to reconcile students to the 'scientific' management of society to make them complacent citizens of technopolis and to identify those considered 'socially undersirable' or 'socially dangerous.'" (quoted in "Sex Educationists Fight God," SJR, Dec. 1971, p. 267)

Beach focuses here upon the use of Sensitivity Training in sex education programs which are deliberately designed to change the attitudes and behavior of children and youth—in the direction, it should be pointed out—*away from the norms of traditional Judaeo-Christian sexual morality.* That modern sex education is of such a character is again strikingly evidenced in a blatantly candid article "Sex Education and the New Morality" written by Chicago Planned Perenthood's Mr. Jerome Becwar in the Nov. 1972 The American Biology Teacher. Like most other sex educators, Mr. Becwar praises a "rational approach to human sexulality": i.e., one which will assure that "sexual activity does not result in the conception of an unwanted child"; where "neither sexual partner

knowingly transmits a venereal disease to the other"; where "neither sexual partner exploits the other as a sexual object"; and which frankly promotes a "relativistic ethics." A "relativistic ethics" is unhesitatingly defined as "one that acknowledges *no particular view of sexual conduct is antithetic to the idea of individual freedom in a democratic society.*" In Mr. Becwar's judgment, Catholics and other Christians who adhere to an absolutist sexual ethic are apparently to be considered enemies of individual freedom and a democratic society!

What appears increasingly obvious is that the tremendous advances in science and technology, and the explosion in the behavioral sciences—psychology, sociology, and anthropology—has resulted in a tremendous contemporary effort to engage the schools in the process of *human engineering*—and this, of course, has all sorts of totalitarian resonances. The triumph of John Dewey's progressivism in American Education has now entered a new phase. Progressivist Liberal educators are now using sophisticated behavioral techniques *to deliberately eradicate all social, economic and sexual inequalities*—through the schools. Schools have the function to change society—to reconstruct society along the lines of the democrat-socialist political model: Teachers assume the mantle of behavioral "change agents" dedicated to unfreezing *those older beliefs and attitudes* which might serve as an obstacle to the implementation of the new, socially-relevant concepts dear to the educationist planners of the National Educational Association (NEA)—perhaps the most powerful lobbying organization in the United States. Their concept of the "new society" bears a startling resemblance to a democrat-socialist political and economic order where a maximum of personal freedom is cunningly publicized by a Leviathan secular State ready to impose population controls and other anti-Christian legislation! Their contradictions are many.

How do educational "change agents" accomplish their purpose of changing human personalities for the emerging technocratic "new order?" They do this by utilizing sensitivity training techniques. These are methods for inducing *planned change*. They are the methods used in group meetings, large or small, conducted by teachers become "trainers" and "clinicians" to publicly discuss intimate and personal matters and opinions, values or beliefs—and to act out emotions and feelings toward one another in a group, using group confession and mutual criticism. Prof. Max Birnbaum, an associate professor and director of Boston University's Human Relations Laboratory, has explained the genesis of Sensitivity Training:

"Responsible for the development of human relations training . . . was Leland Bradford, then director of the Adult Education Division of the NEA, together with his old friend and collaborators, Ronald Lippit, now of the University of Michigan, and Kenneth Benne, now of the Boston University Human Relations Center. . . . Drawing on the work of the great social psychologist Kurt Lewin, they established the first training center more than 2 decades ago at Bethel, Maine, and founded the National Training Laboraotries (NTL). And it was Bradford's tough and dogged fight against strong opposition within education that finally won sanction and support for human relations training, first from industry, then from the social and behavioral scientists, and finally from the educational hierarchy itself. Now, as he is about to retire as director of NTL, Lee Bradford has the satisfaction of seeing human relations training widely embraced by the education world. . . . The trend toward a psychological emphasis appeared in the 1950's when the movement began to attract a large number of people trained in clinical psychology or psychiatry." ("Sense About Sensitivity Training" in Saturday Review of Literature 11-15-69).

Prof. Birnbaum's article is especially interesting for its frank admissions concerning the grave dangers to human personality stemming from the misuse of T-group methods, whose "intense emotional impact" he stresses. Whatever value the T-group may have in improving "the human relations skills of normal people" in industrial and commercial organizations—to improve efficiency and production, he acknowledges that Sensitivity Training can worsen the problems of emotionally-disturbed people. Prof. Birnbaum confesses that where Sensitivity Training is designed to "stimulate the individual's personal growth," the more glaring abuses take place. Serious psychological and emotional damage results when individuals are exposed to disturbing experiences by unskilled and unlicensed quacks posing as therapists.

There are countless incidents like this one recounted in the San Diego Union of Nov. 1968:

"My son is 17. Last night he returned from church in tears. He had attended an 'encounter group' meeting for 'sensitivity training.' The members meet twice a week. They pick a victim for each meeting. Then the members tell him what they don't like about him. My son's friends criticized his manners, haircut, eye color, acne scars, intelligence, vocational plans, clothes, car, and even his parents. They were brutal, and extremely unfair. An assistant minister leads the group. He has had no training in counseling or as a psychologist. The man publicly called my son 'chicken' for getting upset. Do you approve of encounter groups, Dr. Barbour?"

Esalen encounter groups have received a greater measure of notoriety in the mass-media. As Time magazine reported, they can be a "shocking experience."

"People touch, hold hands, kiss, throw each other up in the air, fight, use all the dirty words, tell each other cruel truths. Every aspect of so-called proper behavior is discarded. Every emotion is out in the open—everybody's property. Feelings are not spared. In time, the group develops a tribal loyalty to its own values, as fiercely protective as it is critical." (Time, 11–9–70).

[From the Congressional Record, Extensions of Remarks, Apr. 9, 1974]

RIGHT TO PRIVACY

Mr. RONCALLO of New York. Mr. Speaker, in a decision just 73 years ago, Chief Justice Alton B. Parker of the New York Court of Appeals sounded a contemporary note, commending what we have come to call the right to privacy. "A man," wrote Chief Justice Parker, "has a right to pass through this world, if he wills, without having his pictures published, his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon, whether in handbills, circulars, catalogs, newspapers, or periodicals." Since 1902, the right of the citizen to be alone has been subject to intrusions on a scale which no one could have then predicted or foreseen. Data banks, numerical identifiers, and all kinds of electronic and other means of securing information have flourished, as the psalm says of the wicked, "like a green bay tree."

In his grim novel of Soviet life, "Cancer Ward," Alexander Solzhenitsyn portrayed a society in which the right of individual privacy is subverted and destroyed by the state:

"As every man goes through life, he fills in a number of forms for the record, each containing a number of questions. There are thus hundreds of little threads radiating from each man, millions of threads in all. If these threads were suddenly to become visible, people would lose all ability to move."

It is to prevent anything like this in America that I join with my colleagues today to reflect the growing concern among our people and to demonstrate the congressional commitment to privacy.

There are grave problems in both the private and the public sectors of our Nation. The use and abuse of information gathered by credit organizations, harassment of citizens by telephone and bill collection agencies, and the exchange of personal data among such bodies as banks, hospitals, insurance agencies, credit bureaus, and police are all related to the threat to confidentiality in the private sector. In the public sector there are similar problems, including the gathering and unauthorized distribution of records and other personal data, the use and abuse of national computer data banks, and the collection of information on virtually every aspect of individual life.

In the words of the Massachusetts Special Commission on Privacy and Data:

"This personal information may be collected without the consent of the individual; without provision to check its accuracy: and without control over its dissemination."

Moreover, the growing exchange of such records between governmental and private agencies gives a special urgency to the measures which have been proposed in Congress.

I am proud to be a cosponsor of bills to protect individual privacy in both the public and private sectors. H.R. 6840 would limit the sale or other distribution of mailing lists by Federal agencies. H.R. 8024 provides that individuals on whom Federal records are maintained or augmented be informed of such and have the right of inspecting and correcting the record. Disclosure to other agencies and persons are limited to those cases mandated by law, and the in-

dividual must be informed of such disclosure. In the private sphere, H.R. 10440 sets civil penalties for the use of the telephone to threaten or harass an individual in order to collect an alleged debt or to inform the individual's employer of such allegation. I strongly urge the passage of these three bills and their swift implementation.

One area of governmental concern which is always in conflict with the right to privacy is the census. This is a necessary function of the Federal Government which is mandated by the Constitution. Great care must be taken, however, to prevent the Census Bureau from overstepping their bounds. With this in mind I recently testified before the Subcommittee on Census and Statistics of the House Committee on Post Office and Civil Service regarding an abusive aspect of one of the economic census questionnaires.

[The testimony follows:]

ECONOMIC CENSUS QUESTIONNAIRES

(By Angelo D. Roncallo)

Mr. Chairman, I am delighted to be afforded this opportunity to make this statement to the Subcommittee on Census and Statistics on behalf of H.R. 10510 which provides for Congressional approval of the content of Economic Census questionnaires.

Other witnesses, I am sure, will testify in support of the bill in general, telling you how the Bureau of the Census can and has gone beyond Title 13 of the U.S. Code as enacted by Congress and even further beyond the Constitutional requirement for a census. I think it is important that the full committee and its counterpart in the Senate take back the reins of power in this field and see to it that Congressional intent is complied with by exercising direct oversight of the questions and form of the Economic Census.

Instead of discussing the bill in general, therefore, I wish to concentrate my testimony today on an abuse currently being practiced by the Census Bureau—an abuse which I am confident the Committee would not allow, had it the power which H.R. 10510 would grant. I refer to Form MB–2, which is titled the "1972 Survey of Business Ownership" and requires businesses under penalty of law to reveal the principal source of ancestry of owners, partners or shareholders. I am deeply disturbed at the constitutional questions which this questionnaire raises.

Although the Census Bureau is prohibited by law from revealing information regarding individual firms. I believe that the Constitution is concerned with preventing the possibility of abuse at least as much as correcting present or past infringements on the rights of our citizens. Historically, such information has often been used to discriminate against minority groups. Certainly as long as lists of businesses owned by persons of specific ethnic backgrounds can be compiled by Bureau records—and they have admitted to me that this would be a simple task for the computer—there will always be those who will seek to misuse them.

As their justification for including this questionnaire under the Economic Census, the Bureau has written me that "from the point of better management and budgeting" they decided to fund the survey in this manner, thus replacing a former voluntary survey underwritten by SBA, HUD, OEO, Department of Labor and the Economic Development Administration. In doing so, of course, the survey became anything but voluntary. In effect, the Bureau is saying: you are not Americans, you are hyphenated-Americans, and if you don't believe us, you can think about it in jail.

I would not have any violent objections, were this information solicited on a voluntary basis under another census program. If persons do not mind categorizing themselves in this manner, that is fine with me. Nor, at this time, do I want to get into the propriety of collecting ethnic data in the enumerative population census. But there is absolutely no legal or moral justification for this unwarranted invasion of privacy in the name of economics. This is a social, not economic issue.

The Census Bureau says that they need these statistics to provide the above Agencies with the means to evaluate the success of their respective programs in reaching and helping target clients. This monitoring could be done as easily by each Agency using their applicants as a base through voluntary questionnaires which would enumerate those firms which want to be identified as minority businesses. After all, if they do not want the label, they are not seeking assistance under the various aid programs and are not really a part of the target audience.

There are also procedural problems with Form MB–2, such as forcing a person of mixed origin to identify with only one facet of his heritage. The answer is not to improve the form, however, but to eliminate it entirely.

Mr. Chairman, I feel certain that the Committee would stop this and other unwarrented invasions of privacy if H.R. 10510 were enacted into law. At least every Member would finally be assured of a fair hearing of his concerns on their merits by an objective body looking to protect the public interest, rather than looking to defensively justify previously made bureaucratic decisions. As our oversight committee, you are eminently qualified to represent the House in this area and to see that Congressional intent is complied with.

I respectfully urge the Subcommittee to report H.R. 10510 to the full Post Office and Civil Service Committee so that the bill can reach the Floor of the House at the earliest possible date. Thank you, Mr. Chairman.

Mr. Speaker, ours is the challenge of preserving, protecting and enhancing the right to privacy which belongs inviolate to every citizen, a task which will reaffirm our commitment to individual liberty and the dignity of every person under God. I commend the gentlemen from California (Mr. Goldwater) and my colleague from New York (Mr. Koch) for taking these special orders today. I am pleased to join with them and the other Members who have spoken on behalf of the right to privacy.

[From the Congressional Record, Extensions of Remarks, Apr. 3, 1974]

Right of Privacy

Mr. Rousselot. Mr. Speaker, at this point in this important special order on the subject of the individual's right of privacy, I would like to include the remarks of my colleague, Representative Barry Goldwater, Jr., as he presented them in an address delivered in California recently. The title is "Restoration of Personal Privacy and Individual Rights."

[The remarks follows:]

Restoration of Personal Privacy and Individual Rights

(Address by Representative Barry M. Goldwater, Jr.)

The pursuit of human liberty and dignity brings us together today. In this vital cause, let us call on all Americans to join a crusade for personal privacy. In this spirit, I want to share some ideas and insights today.

Awareness of gradual, but growing intrusions on personal freedom is spreading rapidly. Civic and patriotic groups, the academic community and many Members of Congress have the commitment. We are on the attack and we will succeed!

Nothing short of a national battle plan must be formulated in Congress and by state governments to reverse the insidious denuding of every person's personal privacy and individual rights. Furthermore, the ability of the government and big business to indiscriminately exchange private information about any individual must be stopped.

ZONES OF PRIVACY

I am concentrating on the area of information protection, sometimes termed data surveillance. This is not to suggest I am unaware of other forms of privacy invasion. All too many forms of violations of personal liberty can be found in the current news:

Watergate was an invasion of privacy.

The break-in of Dr. Ellsburg's psychiatrist's office was an attack on privacy.

Unwarranted wiretapping and physical surveillance are intrusions of privacy.

Behavioral modification of small children or persons in penal institutions invade personality and individuality.

Similarly, collecting sensitive personal facts about individuals, handling it in a careless or inaccurate manner, selling or transferring files without the consent of the giver, these too are invasions of privacy.

GROWING CONGESSIONAL COMMITMENT

For almost a decade, a few isolated voices in Congress and throughout America have proposed remedies to privacy invasion. The commitment has been slow in coming, but I see real signs of its arrival. I point to recent adoption by the House

of my privacy amendment to the Federal Energy Administration bill. To the best of my knowledge, this was the first time an amendment of this nature was included in a measure establishing a new agency of the federal government. The amendment requires the agency to protect and assure the privacy of personal information collected or used by the Administration.

It also requires the Administrator to establish guidelines and procedures for handling individual identifiable personal data.

I pledge to offer more privacy amendments. When legislation comes to the House where information on individuals is involved, specific guarantees of confidentiality must be included. If privacy is ignored, I will make privacy requirements heard!

CONTROLLING DATA SURVEILLANCE ACTIVITIES

As we think of the concept of privacy in the modern context, it means protected rights of personality. Privacy is invaded when an individual is required to divulge sensitive personal facts about himself.

This may be in answer to a government questionnaire, applications for assistance or any type of information collecting requirement. If personal information sought conforms to minimum needs, privacy is less threatened.

Once personal information enters a record system, its confidentiality must be protected. This is the case if the information is used only for the purpose it was taken, and data managers take care for its accuracy and validity. Once the need for this information has ended, it is the duty of the users to halt further transfer or release of the data, and in accordance with a specific policy, purged from the system.

There are four reasons for the call to privacy action, each supported by the fact this prudent attention to private rights has not been respected. Excesses by government and private data collectors and users are alarming the public. This has escalated due to unresponsiveness and insensitivity to individual concern over personal files. Technological innovation has magnified the privacy dangers, because of automation of information handling. Collection, processing, and analysis by computers and telecommunications give new dimensions to manual methods of record keeping.

Public understanding of this threat to their civil liberties has elevated privacy as a priority national problem. Confidence in government has fallen, and in part because of distrust in government information practices.

THE CONCEPT OF PRIVACY

To more clearly understand the practical and philosophical basis of this attack on personality, let us look to our Western development of man, and of social order from three centers. They are Jerusalem, Athens, and Rome.

The idea of society and of community in the presence of God came from Jerusalem. The Greeks gave us reason and philosophy—the systematic search for knowledge and truth.

Socrates, Plato, and Aristotle believed that social order is founded on human person, on human relationships and actions. The state, then, had the necessity to reflect the order or chaos of the citizens' inner lives, which could be seen in their outward lifestyle.

Some of the ancient Greeks, notably Plato with his *Republic*, were seeking perfect wisdom and justice.

But these philosopher kings have never really existed. The Greeks conceived a State founded on law. At that time, a main objective of law was to restrain the rulers. Law was to substitute for fear and coercion as the means for ruling. It was meant to lead men to the cultivation of virtue, to insure liberty. This required raising common interests above special ones. Law was to correct injustice and to educate men to love justice.

The concept of privacy as a human value began in these early times. The individual was the basis of society, a social order based on laws, where men were seeking knowledge, truth and justice. Religion also played an important part in developing the concept of privacy.

IMPORTANCE OF LAW AND RELIGION

Greek and Roman law evolved from family custom. The family was rooted in its land, the land of their ancestors and which supported the family.

This is more clearly described among the Romans. Cicero asked, "What is there more holy than the house and the land of each individual citizen? Here is his altar, here is his hearth, here are his household gods. Here all his sacred rights, all his religious ceremoneies, are preserved."

These were the origins of our own sense of "patriotism." Literally, patriotism meant love of the land and love of our fathers.

Religion was vitally important to understanding the ancient family and the society which evolved from it. From it was established marriage, paternal authority, and fixed relationships. The rights of property and inheritance were consecrated during these times. This is the same religion, after having engaged and extended the family, that formed a still larger association: the city.

The city was to be ruled in the same manner as the family. From it came all the institutions as well as the private law of the ancients.

Then, the importance of the family and family love became badly distorted. Instead of one individual, and one family being foremost, a new political life was created—the ruler. This was the father image raised to the level of hero or god.

We must not overlook the principles these Greeks and Romans left us. The law, respect for the family, and patriotism number among them. Omitted, however, was moral and ethical direction for the state.

EARLY CHRISTIAN INFLUENCES ON GOVERNMENT

Christianity has done much to fashion the politics and forms of government of Western history. St. Augustine brought together Mosaic law, Socratic philosophy, and natural law. He believed that a state and the politics of a people should reflect the society's understanding of themselves. With moral and ethical direction he called for a hierarchy of ends, putting aside the unimportant.

We should seek the highest ends, according to St. Augustine. These higher goals followed moral precepts and by following such objectives, St. Augustine believed a person's life would be marked by charity, love and freedom.

THE DOCTRINE OF FREEDOM

The doctrine of freedom is essential to privacy. Freedom to obtain ends beyond mere things—mere materialism. Freedom to pursue higher ends. But to do this we must have free well. All of these early concepts are falling into place. The importance of the *individual and family*, the *creation of laws* as a substitute for fear and coercion. To seek higher goals, we must have *free will*, and *free choice*.

There are enemies of freedom as we well know. Perhaps the greatest ones lie within ourselves: fear, desire, and ignorance. Forces outside ourselves appeal to our fears. We know of people who have sold their freedom for money, security, position. Here is the key blunder of people who will use freedom to gain short run benefits. These misled people think freedom is not a spiritual or intellectual quality, but a material one.

This materialism blunder can easily lead to the view that men with more *things* are bound to be somehow freer and happier than men without them.

Such a notion has been important to the development of our modern technocracy. Life today is based on a system for the production and consumption of things in ever-expanding quantities. We might ask ourselves if a man with everything is freer than a man with nothing?

LOSING OUR DIRECTION

Where and how did we lose our way? Our short historical review shows we lost our way we gave so much importance to material values, and not human ones.

We have placed *material security* over *intellectual freedom*. We let big government take over our *personal responsibilities*, and those of our churches and charities. We let government educate us, house us and direct our cultural experience.

Now, we wonder why this collapse in our rights to be left alone, after we have permitted, and even *asked*, the government to do it for us.

Our generation worships social utility, and the rationalism so prominent in science today. Science, like all philosophy, *had* been dedicated to the search for wisdom. Now the scientists do not seek simply to understand nature, but try to control it.

37-583 O - 74 - pt. 2 - 31

THE MATERIALISTIC CONCEIPT OF MAN

Science and technology are justly credited with giving us bountiful progress, and in large measure this has been to our advantage. However, I think we must look again to see if all the new methods and apparatus for development are making us slaves to new masters.

Are not many of these political and social techniques to regulate the flow of all goods and services really controlling our choices and opportunities?

This is the modern economic view of man. Every television commercial underscores the consumer society. We are told we will be happy and satisfied if we have enough *things*. Moral qualities are irrelevant.

This economic view of man dominates our lives! By itself, it is an immoral view. I submit this kind of concept of man motivated the Nazis who propelled it to a horrible zenith. Unfortunately, these notions explain much of the modern world.

TECHNOCRACY OR TECHNOLOGY

I want to state here and now that I am not launching an attack on technology as such. There are really two concepts: technology and technocracy. There is the one that stands as a kind of intermediary between men and their environment. This has produced the club and the wheel, and is neutral in the molding of human destiny. Technocracy is the product of that applied science which evolved when the scientists, infected by rationalism, sought to cure the ills of the world. They developed solutions which they believed would erase suffering, end hunger, provide riches, and generally secure everyone's welfare. This is the claim that suffering, hunger, and poverty could be abolished by an act of will, or more precisely, by government money.

It is this technocarcy that limits freedom. For in a technocracy, men must choose only the most efficient techniques to achieve desired ends, to the detriment of every other standard, like beauty or humanity. Determining the most efficient means for a project requires an accumulation of facts, then more facts, to explain the ones already collected. So many facts that techniques of fact-finding and collecting have become a special field of development. The accumulation of facts, the collection of data, becomes so vast an enterprise that ordinary logic cannot embrace it. The computer has spawned the "technical mind." This is a peculiary 20th century phenomenon.

Lines of verse or the lines of a painting may differ, but facts once established will not. So with the technical mind, unlike the poetical or artistic, every technical mind is just like every other technical mind.

This means that one man with a technical mind is as able as every other man with a technical mind. It says that one man with a technical mind is as able as any other to do a technical job. Everything distinctive, individual, or superior in terms of qualities of a man's mind is not relevant.

Everything centers on the quantitative; down with qualitative dimensions or values. If there are no jobs except technnical ones, everyone will function according to the same common, and may I say low, standard.

THE CYBERNETIC STATE

Another result of the vast accumulation of facts is that it makes for an extremely complex society. This is technocracy. Will it function according to the will of the public? No. Can the mechanisms of society be operated by bureaucrats? No. Only *technocrats*.

Since ours is becoming an essentially mechanical state, it is vital that all its parts operate smoothly. If the flow of mail in one area is interrupted, it is enough to declare a national emergency and call in the Army. This was actually done during the mail strike a few years ago.

If some scheduled air flights are disrupted by criminal hijackers, it is enough to subject all of us to a close search. We probably take the search for granted, as if we never travelled freely. Here we are getting to what is the overall meaning of my message today.

My concern has to do with our reasons for surrendering to the tyranny of technocracy. For there is no question we are surrendering.

And what I am talking about is *tyranny*. As our country has been mobilized into a technical society, the more we have become technocracy's servants. We have been asked again and again to place technical accomplishment at the top of our list of human values. Technocracy requires order, as absolute as possible.

Here we have one of the root causes of society's demand to apprehend and punish those who disrupt order. A penchant for order has blinded people to overlook the purposes prompting disorderliness. A student demonstration is reported largely for its disorderly characteristics, almost overlooking the motivations of the participants.

I am not condoning disorders, or disorderly conduct. But I am suggesting that society is often missing the point by worshipping order.

Our need for order has led us to appeal to the technicians, to lead the search and to devise the means, the techniques, to effect change. The state becomes not only the main source for the development of the techniques of social control, but its agencies are also the chief beneficiaries of the techniques. Guarding against the evolving technobureaucratic establishment must be a great challenge to all of us.

PROGRAMMING THE PROGRAMMERS

We have traced a long historical road today . . . leading to 1984 and beyond. We must defang Big Brother. We are the generation to withstand Future Shock. But I trust you will not think I am speaking about an alarmist's flight of fancy. The computer-telecommunications era is already upon us.

There are currently 150,000 computers in use in the United States, and some 350,000 remote data terminals. Predictions have been made indicating there will be 250,000 computers and 800,000 terminals by 1975. Revolutionary changes in data storage are taking place.

It is possible today to build a computerized on-line file containing the compact equivalent of 20 pages of typed information about the personal history and selected activities of every man, woman and child in the United States.

In this system any single record can be retrieved in about 30 seconds. Few can deny that we are appraoaching a data bank society. My objective is not to undo or slow down technical advancement, but rather to put men *over* machines.

Let us insert private rights into the programs of the programmers. Let us restore human dignity as the cardinal principle, rather than worship the gods of efficiency and economy. We must manipulate the manipulators.

The dehumanists of technocracy should have the back seat in the reshaping of our destinies.

THE CONGRESSIONAL COMMITMENT

There are now more than 300 members of the United States Congress, both House and Senate, who have sponsored one or more of the 60 different approaches to restoring rights of privacy of Americans.

Each of these different remedies strikes at a particular evil or abuse. What is really needed is a broadly framed measure incorporating the best solutions. It must include all kinds of information collection practices, whether maintained on computers or intraditional filing methods.

Private organizations and businesses must be required to conform to these standards. Fortunately, a recent Department of Health. Education and Welfare Advisory Commission Report on Automated Personal Data Systems set out good recommendations for a Code of Fair Personal Information Practices.

I was given the opportunity by Secretary Weinberger and former Secretary of Justice Elliot Richardson to introduce legislation implementing the report in the House.

The basic proposals of this legislation are:

There must be no personal data system whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record, and how that information is to be used.

There must be a way for an individual to correct information about himself, if it is erroneous.

There must be a record of every significant access to any personal data in the system, including the identity of all persons and organizations to whom access has been given.

There must be a way for an individual to prevent information about him collected for one purpose from being used for other purposes, without his consent.

EXECUTING THE BATTLE PLAN

This is a bi-partisan, patriotic, and civil liberties issue. I am glad the President has called for a review of this situation, by way of a four-month study directed by Vice President Ford.

I met with the Vice President earlier this month in Washington, and suggested that instead of merely studying the issue further, the committee should take the best ideas from government reports and congressional proposals. These should be sent to the Congress, with the endorsement of the President, before July.

We have before us a unique opportunity to make the 93rd congress the Right to Privacy Congress.

Should we fail to seize this challenge now, and act upon it, the spectre of technological tyranny will become reality.

[From the Congressional Record, Apr. 4, 1974]

THE AMERICAN RIGHT TO PRIVACY

Mr. STOKES. Mr. Speaker, President Nixon has belatedly recognized that privacy exists, Nixon's deeds more than his radio statement make a strong case for increased protection for the right to privacy. Privacy is a vital national concern which must receive increased attention if it is to be preserved against the onslaught of technology and bureaucracy. An excellent response to Nixon's radio statement on privacy was made by Aryeh Neier, executive director of the American Civil Liberties Union:

[The article follows:]

RESPONSE BY ARYEH NEIER, EXECUTIVE DIRECTOR, AMERICAN CIVIL LIBERTIES UNION, TO THE ADDRESS BY PRESIDENT RICHARD NIXON DELIVERED ON FEBRUARY 23, 1974, "THE AMERICAN RIGHT OF PRIVACY"

Last Saturday, President Richard Nixon said that if government "fails to respect its citizens' right to privacy, [it] fails to respect the citizens themselves." Most Americans would agree with that statement. It is good to see President Nixon expressing such sentiments. While there is a certain irony in the fact that this President made that statement, anyone devoted to the right of privacy can only welcome the President's profession of concern.

Unfortunately, there was a glaring omission from the President's statement. It is so significant and remarkable an omission that it is difficult to believe it was accidental. The President rightly noted that, "Careers have been ruined, marriages have been wrecked, reputations built up over a lifetime have been destroyed by misuse or abuse of data." However, he discussed these problems entirely in the context of data-banks created for the collection and dissemination of information for consumer credit, social welfare, insurance and criminal justice purposes. At no time did President Nixon so much as mention the problems of political surveillance. Furthermore, there was no hint of concern with political surveillance in the detailed background paper that was issued in conjunction with President Nixon's speech by the Office of the White House Press Secretary.

The problem of political surveillance has been highlighted by the Watergate disclosures of the past year. However, it is not a new problem. For more than a half century, the Federal Bureau of Investigation has been collecting data on persons engaging in lawful political activity. The F.B.I. infiltrates peaceful political organizations, photographs participants in lawful demonstrations, peruses the bank records and tax returns of political dissenters, records their names and exchanges inteligence data with many other governmental agencies. A deliberate purpose of this activity, as an internal Bureau memorandum has instructed agents, is "to get the point cross that there is an F.B.I. agent behind every mailbox." Such other federal government agencies as the Immigration and Naturalization Service, the Department of Health, Education and Welfare, the Passport Division of the State Department, the Secret Service and the intelligence divisions of the various military services have all compiled banks of dossiers on political dissenters. In addition, most urban police departments have had their own political surveillance systems.

In a recent court case, the New York City Police Department admitted that it alone had maintained files on the peaceful and lawful political activities of about a million persons. Political data banks are also maintained by Congressional committees and by private agencies which make a business out of selling this information to employers.

Surveillance of lawful political activities is often justified by the claim that its purpose is to protect our national security. The shibboleth of national security

is also invoked as the reason for keeping secret from the American public many of the activities of its government. It is high time to abandon these claims of national security. We cannot achieve security by methods which destroy the basic freedoms of the society we seek to protect. A functioning democratic society cannot endure unless its citizens can engage in political activities free from an all encompassing sense of being observed and recorded. The tone of life and spontaneity or spirit which should characterize a free society cannot survive in an atmosphere in which a person's every deviation from the political norm is noted by government snoopers and stored for future reference. The consequence of such intensive monitoring of political activities and associations must inevitably be the drastic curtailment of any society's capacity for diversity and freedom.

For the most part, this country's political surveillance apparatus has grown up in the absence of any legal authority to support it. It has appeared to have a life of its own and our elected officials seem unable to control the snoopers in the F.B.I. and in the other agencies which gather domestic political intelligence. It hardly seems possible to engage in a serious effort to reestablish the right to privacy if the entire question of political surveillance is evaded, as it was evaded by President Nixon in his speech last Saturday.

In the areas that he did touch upon, the President made a number of commendable comments. He noted that credit is often withheld on the basis of inaccurate data; that jobs may be denied because of arrest records not updated to show that charges were dropped or the person found innocent; and that what a person gives to his church or his charity is his own personal business. To deal with these problems, President Nixon said, "We need more than just another investigation and just another series of reports." Quite right. However, the President failed to note that there are bills presently pending in Congress which effectively address all these problems and other pressing problems vitally affecting the right to privacy. Among these bills are:

Senate bill 2360—This bill which was introduced by Senator William Proxmire, would reform the practices of the credit industry by requiring agencies seeking a report on a person to obtain his or her consent. It would also give the person about whom a credit report was compiled the right to inspect and obtain a copy of his or her file; require expungment or correction of incomplete information limit disseminations to those authorized by the subject of a report; and ban the collection of data about political views, race, religion, and of uncorroborated hearsay.

Senate bills 2963 and 2964 which were introduced by Senators Ervin and Hruska and House bill 9873 introduced by Representative Edwards would severely restrict the dissemination of arrest records not followed by convictions and would limit the wholly promiscuous dissemination of conviction records.

Senate bill 2200 introduced by Senator Cranston and House bill 9424 introduced by Representative Stark would require formal legal process or customer permission when the government tries to examine an individual's bank records.

Senate bill 2810 introduced by Senator Goldwater and House bill 10043 introduced by Representative Barry Goldwater, Jr. would place important controls on government data banks returning control over personal information to the individual to whom it relates.

Senate bill 2820 introduced by Senator Nelson would eliminate all wiretapping that is not, at the very least, authorized by a warrant granted by a court.

Senate bill 2318 introduced by Senator Ervin would prohibit the military from spying on civilian citizens.

A number of these bills have wide support in the Congress. For example, Senator Ervin's bill to ban political surveillance over civilians by the military has 34 co-sponsors in the Senate. Support for such specific measures from the President could help greatly in getting them adopted. If President Nixon means what he says when he states, "We need action," he should lend his support now to such specific measures. Unfortunately, that is not what the President has yet done. While he stated that we need "more than just another investigation," he has set in motion just such an investigation. President Nixon has created a Committee of government officials chaired by Vice President Ford to tackle the problem of privacy. He has directed that Committee to begin to provide a series of measures to protect privacy within four months. If the Committee follows the President's directions, it should be ready to begin proposing measures by the end of June. That will be close to the time that the Congress will adjourn for the summer in this, an election year. In all likelihood, it would mean no Congressional action at all in 1974.

Despite shortcomings, President Nixon's expressions of concern about privacy are a very valuable contribution. I urge the President to make good on the concerns he has stated. He can do so by giving timely support to some of the specific measures to protect privacy now pending in Congress. And, perhaps even more significantly President Nixon can do so by enlarging his horizons to encompasse the most serious of the many intrusions on the right to privacy; the problem of political surveillance. If we cannot keep our rights to speak and associate from being noted and recorded by Big Brother for possible use against us, then the right to privacy will not exist.

[From the Congressional Record, Extension of Remarks, Apr. 15, 1974]

LOCAL PHONE COMPANY SETS NEW POLICY ON GIVING DATA TO POLICE

Mr. OBEY. Mr. Speaker, the Wood County, Wis., Telephone Co. has decided it will not turn over long-distance call records to law enforcement or investigative agencies except under subpena or administrative summons.

The company will also notify those customers whose records have been subpenaed, unless the agency involved certifies to the company that notification "could impede its investigation and interfere with enforcement of the law."

I think the Wood County Telephone Co. should be heartily commended for adopting this policy to protect individual privacy against informal snooping by Federal, State, and local agencies.

Here is an article from the Wisconsin Rapids Tribune of March 29, explaining how the policy will work and why it was adopted:

[The article follows:]

[From the Wisconsin Rapids Tribune, Mar. 29, 1974]

PHONE COMPANY HERE SETS NEW POLICY ON GIVING DATA TO POLICE

(By Thomas Berger)

Effective immediately, the Wood County Telephone Co. will not turn over long distance telephone call records to government or law enforcement agencies of legislative committees except under subpoena or administrative summons, the board of directors of the company decided Thursday.

In the past the company honored requests from local law enforcement agencies for records of toll calls. The information included date, time, duration and number called.

James Wenzlaff, vice president and general manager of the company, refused comment on other agencies the information was released to or the number of requests received or honored.

He said he had heard news reports of other telephone companies giving the information to the Internal Revenue Service, the Federal Bureau of Investigation and the Department of Justice but refused to say if the Wood County Telephone Company had also surrendered records to the agencies.

Wisconsin Rapids Police Chief Allen Spencer and Wood County Sheriff Thomas Forsyth both said the information was requested by their agencies only very infrequently.

The company will also now begin notifying customers when their records have been subpoenaed or summoned, except in those circumstances where the agency requests the company not to disclose that information and certifies such notification "could impede its investigation and interfere with enforcement of the law."

Until now customers were informed of a subpoena or summons only if they asked whether such action had taken place, the company said. Now the person whose records are sought will be notified by a phone call and a letter written within 24 hours.

Wenzlaff said the company will no longer honor a demand for such records in the form of written requests from law enforcement agencies.

Spencer said he could not recall the last time such records were requested by Wisconsin Rapids police. Forsyth said the last time his department did was "about two years ago on a drug case."

"The FBI used to use this type of thing a lot," Forsyth said. "We have done this but on such rare occasions."

The company's officials met with Spencer and Forsyth about three weeks ago to discuss the changes in the company policies. "The company also will no longer give police an unlisted number, even in case of an emergency," Forsyth said.

"We have reviewed our policy in the all-important area of customer privacy many times over the years and these changes are the result of the latest such review," Wenzlaff said. "There are important issues involved—the right of individual privacy is vital and so is the need for effective law enforcement.

"We are deeply concerned about the need to protect individual privacy. We would prefer not to reveal anything to anybody about the billing records of our customers, but obviously we must honor subpoenas served upon us."

He said that only the information necessary for billing purposes was surrendered and "These records contain no information as to the contents of any telephone conversation."

He refused comment when asked whether the company has allowed any taps to be placed on its telephone lines.

A bill has been introduced into the Wisconsin Assembly's Judiciary Committee requiring investigators to get court permission to explore utility records of calls. Wisconsin Telephone Co. disclosed last year it provided the Justice Department with records of toll calls but discontinued the practice March 1 this year.

[From the Congressional Record, Extensions of Remarks, Apr. 9, 1974]

RIGHT TO PRIVACY

Mr. ESCH. Mr. Speaker, many Members of Congress have been looking forward to adoption of legislation to place tight controls on criminal information systems in order to protect individual privacy. House and Senate subcommittees have held public hearings and hopefully within the next several months we will see final committee action on this very complex legislation.

I believe adoption of this much-needed legislation must be accomplished during this session of Congress, especially in view of the many timely warnings about the risk of unwarranted encroachment on individual privacy by unchecked use of computers to compile crime records.

The following article by the Long Island, N.Y., Newsday, provides a wealth of information about the increased use of computers for the collection and dissemination of arrest records. It notes, for example, that the FBI expects to have records of 1 million persons on file by 1984 which could be sent upon request to 40,000 local police departments in a matter of seconds.

Obviously, computerized information systems have enormous potential for increasing the capability of law enforcement. However, we must balance a concerted tough attack on organized crime and street crime with the kinds of safeguards that will protect the right to privacy that all of us should enjoy as citizens of the United States.

For that reason, I hope the Congress will continue to give this matter most thorough consideration so that later this year we can develop the kind of effective legislation that is so much needed.

[The article follows:]

FBI TO STORE ARREST RECORDS OF 1 MILLION

WASHINGTON.—By 1984, the FBI expects to have stored away in computers the arrest records of 1,000,000 persons. Those records will be available to 40,000 local police departments through a telecommunications network capable of locating a file and sending it across the country in less than five seconds.

More quickly and completely than ever before, the system will send out descriptions of wanted persons, of stolen cars and stolen securities. Law enforcement officials across the nation will have almost instant access to the criminal records of any person they want checked.

There is concern in the Congress and elsewhere that the rapidly growing system, which was started in 1971, be tightly controlled to insure that the information it provides with such efficiency is both accurate and complete.

That concern has grown in the past decade with the hundreds of disturbing stories about the efficiency of the government's information system.

Consider:

The former Marine deserter from Texas who has served his military prison time and been discharged, but who reportedly has been picked up and detained by police three times in the past year alone because the computer still lists him as a "wanted" man.

Paul Cowan, of Boston, who was issued a taxi driver's license in February, 1971, only to have it revoked one week later because a check with the FBI showed

that he had been arrested for possession of marijuana, but failed to show that the charge had been dismissed.

Sam Ervin of Morgantown, N.C., who opened his mail one morning in 1968 and found that the Social Security Administration had sent him a $752 check labeled "death benefits." To all appearances he was not only alive and well but running for re-election to the United States Senate. It was at that moment that he lost any faith he may have had in the infallibility of computers in general and government data banks, in particular.

Ervin also happens to be the chairman of the Senate's subcommittee on Constitutional Rights, and will chair hearings next month on two bills—including one of his own—to limit the uses of information in criminal data banks.

The Ervin bill grew out of four years of investigation by his subcommittee, during which Ervin became an increasingly vocal critic of government intelligence-gathering and the poliferation of data banks. The senator warned of the erosion of the right to privacy, a right not specifically mentioned in the Constitution but clearly implied.

The concern about criminal data banks has grown as the FBI and local police have begun converting from file-drawer record systems to an interlocking network of computerized data banks.

The FBI, which has arrest records on about 20 million persons in its manual files has computerized about 500,000 arrest records, and expects to have computerized 8 million of them within a decade.

To Ervin, the "benign inefficiency" of the file-drawer systems has prevented them from becoming "an intolerable threat to personal privacy or reputations."

But now that information is being computerized and exchanged with thousands of other state and federal agencies, he fears that neither the citizen nor the government will be able to control "who can see the information . . . or the accuracy of what is broadcast."

It is not just criminals and accused criminals who wind up in government data banks.

John Shattuck, an American Civil Liberties Union attorney, told a federal panel that many ordinary citizens become the subjects of government files as agencies increase the collection and dissemination of "dossiers on citizens engaged in exercising their rights of free speech . . . Medical and welfare records of the disadvantaged (and) the aging . . . Bank records of persons depositing funds in federally insured banks; (and) anecdotal records about children and young adults at every stage of the school system . . . "

No one knows for sure just how many government data banks exists, but they include the Defense Department's dossiers on 1,600,000 civilian employees of defense contractors, the Secret Service's files on 69,000 Americans considered potentially dangerous to the President, and the National Institute of Mental Health's files on persons who have taken part in federal drug treatment programs.

Ervin, who was concerned about privacy long before Watergate, had hoped to author a bill regulating all types of government data banks before retiring from the Senate at the end of this year.

He decided to focus only on criminal data banks after his staff—which identified 750 federal data banks before it stopped counting—found itself unable to draft a bill comprehensive enough to cover them all.

Ervin's subcommittee will consider both his new bill and one originally proposed by Elliot Richardson when he was attorney general. It is being sponsored in the Senate by Sen. Roman Hruska (R-Nebr.) and cosponsored by Ervin. (The Nixon Administration has allowed the bill to be introduced, but has not formally endorsed it.)

Both bills would cover virtually every criminal data system in the country. They would give citizens the right to inspect their own files and to correct any inaccuracies; forbid non-police agencies access to the files, unless a specific state or federal law were passed to permit it, and drastically limit the use of arrest records that do not tell the disposition of the case.

[From the Congressional Record, *Extensions of Remarks, April 11, 1974*]

RIGHT OF PRIVACY

Mr. ANDREWS of North Carolina. Mr. Speaker, it seems inherent in legislative bodies that members react to crises rather than prepare in advance for problems that can be foreseen and anticipated.

In this respect, I fear that our Congress is again guilty on not having enacted sufficient legislation guarding our citizens rights of privacy. Such legislation is past due in our Nation.

Yet, even as we continue to delay our response to this need, there is emerging the need to deal with the complex problems posed by multinational computers and data banks.

This matter is discussed in the January 16 issue of Computerworld in an article by Mr. E. Drake Lundell, Jr., and at this point I would like to insert this into the Record in connection with the special order on privacy arranged by my distinguished colleague, Hon. Edward I. Koch, and others:

[The article follows:]

MULTINATIONAL DATA BANKS REQUIRE SPECIAL SAFEGUARDS

(By E. Drake Lundell, Jr.)

MONTVALE, N.J.—As multinational data banks become more common, "new institutions will be required at the multinational level to resolve disputes over the transmission of data across national boundaries," according to a recent publication from the American Federation of Information Processing Societies (Afips) here.

In addition, the publication said these new institutions would have "to develop regulations concerning the activities of multinational data banks, to provide individual safeguards, and to deal with problems of standardization of data transmission facilities and capabilities."

The publication, written by Burt Nanus of the University of Southern California, Leland M. Wooten of Southern Methodist Universtiy and Harold Borko of the University of California at Los Angeles, is based on the admittedly imperfect Delphi technique, but represents, the authors said, a first attempt at coming to grips with the problems likely to be raised by multinational computers and data bases.

TIME IS COMING

"The use of computers in this manner at the present time is certainly not widespread," the authors admitted. "However, as one projects ahead 10 to 20 years and contemplates, on the one hand, the rising tide of multinationalism in both corporations and governmental organizations, and, one the other hand, the rapid increase in capabilities and decrease in cost of computer/communications networks, one can conjecture it is only a matter of time (and probably not very much time) when these kinds of applications will proliferate."

Within the next 10 years there will be some major multinational networks in existence, the group predicted, but added the nature of the impact of such development is "still only vaguely perceived.

"On the technical side, there appear to be few barriers to the development of these systems that are not now already close to solution," the report noted.

"The problems that do exist are more in the nature of political or socio-cultural," the report added, indicating the most profound effects of these systems will be on this level.

MULTINATIONAL DECISIONS

"Within the highly industrialized societies, many people will find themselves in some form of man-machine relationship, often involving multinational communications, within the next decade," the authors predicted, which might lead to situations where "individuals will be asked to make decisions in a multinational context that may not be consistent with the policies of their own governments."

At the same time the group predicted that while in the short run the use of multinational computers might tend to enhance the prospects of the "information-rich, wealthier nations at the expense of the information-poor," in the long run the use of such systems will increase the "technological options" open to the lesser-developed countries and "speed their ability to industrialize and to take advantage of the latest developments in education, management, medicine or public administration.

"The danger to the devloping nations is that the MNCs (multinational computers) may distort their investment priorities or lead to policies that favor multinational as opposed to national patterns of socio-economic change," the group said.

DELPHI TECHNIQUE

The Delphi technique polls a selected group of people—in this case from several different disciplines, with a series of questionnaires, each succeeding one based on the previous and developed in order to refine the opinions expressed there.

In this group it was found that 50% of the people (all of whom were familiar with computers) felt that multinational computer systems would help "to enhance the power of multinational organizations whose interests transcend national interests and which are generally the creatures of the industrial nations.

In all, 83% felt the use of computers across national boundaries "will contribute to homogenization of cultural values and attitudes," and 60% agreed "the use of computers across national boundaries contradicts the present trend to put 'people' ahead of things."

In all, 83% of the group agreed that political considerations were the most important barrier to the growth of multinational computer systems and 59% said the lack of political or legal mechanisms to determine who controls such data banks was the most important political considerations.

MINOR BARRIER

However, 56% indicated the refusal of nations to lower restrictions on the trade of computers was a relatively unimportant barrier to the growth of multinational systems.

Afips also outlined five areas where future policy is necessary:

"It is likely that the right to individual privacy vis-a-vis the use of various forms of information technology will have to be defined in terms that provide safeguards to individuals in different cultures. That is, the cultural determinants of this right must be transcended in order to adequately protect the right of privacy at the global level.

"Organizations and nations will need a common understanding regarding the fraudulent uses of data by multinational organizations. Protection against these fraudulent uses of data must be safeguarded at the global level.

"Nation-states are likely to begin to formulate policies that enlarge the public arena of control over the use of MNCs.

"Multinational organizations will need to formulate policies regarding the access to information contained in multinational data banks and information systems.

"Multinational organizations and nation-states will need to agree on policies strengthening the position of the LDCs (lesser-developed countries) in all arenas where the use of MNCs is prevalent."

[Prism, June 1974]

MUSHROOMING MEMORY BANKS, ELECTRONIC SURVEILLANCE SYSTEMS, AND COMPUTERIZED DOSSIERS THREATEN TO MAKE US . . .

A NATION OF DATAMANIACS

(by Arthur R. Miller, LL.B.)

The Author: A professor of law at Harvard University, Arthur R. Miller is the author of *The Assault on Privacy: Computers, Data Banks and Dossiers* (1971). He has appeared as an expert witness before numerous United States subcommittees to testify on various aspects of computers and privacy and has served with several federal and state commissions drafting legislation on the subject.

Americans today are scrutinized, measured, watched, and questioned more than at any time in their history. This increase in data gathering, combined with ever-broader applications of information technology, understandably has caused growing anxiety over the erosion of our physical and informational privacy. One major concern is that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been into it, may become the heart of surveillance system that will turn society into a transparent world.

A brief recital of some of the blessings and blasphemies of this new technology should bring the computer-privacy dilemma into focus. In several medical centers, doctors are using computers to monitor physiological changes in heart

patients. The quest is to isolate those alterations in the body that precede a heart attack in order to establish an "early warning system" so that treatment need not be delayed until the actual heart attack has rendered the patient virtually moribund. Similarly, the use of Automated Multiphase Health Testing to facilitate diagnosis is becoming more common.

Other plans include giving everyone a standard identifying number at birth for computerizing tax, banking, education, social security, military service, etc. The immediate goal is to eliminate much of today's multiplicity in record keeping. Long-range objectives include developing a checkless, cashless economy, improving information available for rational planning, providing better governmental service to people, and promoting more equitable allocation of society's resources.

Someday in the future, when a traveller falls ill far from home, a local doctor may be able to input the patient's identification number into a desktop computer terminal and retrieve his medical history and drug reactions from a central data bank.

On the opposite side of the ledger, the same electronic sensors that might warn us of an impending heart attack could be used to track our movements measure our motions and thoughts, or modify our behavior. Major breakthroughs in telemetering are on the horizon that may make Michael Crichton's *The Terminal Man* a less bizarre work of science fiction than we might like to think. Some criminologists (apparently oblivious to civil-liberties concerns) already have suggested that a prisoner be subjected to sensor implantation as a condition of parole. He could then be monitored and returned to custody should his "aggression level" become "too high." But how will law enforcement agents distinguish between an elevated aggression level that precedes a burglary and one associated with watching a football game?

A VIRULENT DISEASE

The official identification number might become a leash around our necks and subject us to constant monitoring, making credible the fear of the fabled womb-to-tomb dossier. In an information-based society, those who control our personal data will have a degree of power over us that is constantly subject to abuse. Even seemingly benign commercial uses of cybernetics may cross the line that separates efficiency on the one hand and manipulation on the other. One firm already is developing a comprehensive data bank on doctors, so that drug companies can promote their products in a way that appeals to the habits and personalities of individual practitioners.

An evaluation of information technology's impact on personal privacy is especially appropriate today because of the clarion in all quarters for the establishment of data banks. (See the article by Senator Sam J. Ervin, Jr., on page 14.) As we look to the future, it is certain that the hypnotic attraction of digital record keeping will continue to envelop our universities, corporations, hospitals, and other social institutions. Datamania appears to be one of contemporary society's most virulent diseases.

Without doubt, most data-gathering activities are well-intended efforts to achieve socially desirable objectives. In the law enforcement field, file building is said to be necessary to fight organized crime and restore "law and order." The FBI and the Army justify their intelligence operations in terms of combating subversion or quelling disorders on campuses and in our urban centers. Credit grantors, private investigators, and insurance companies claim that it simply is good business to know as much as possible about someone before you lend money, employ, or insure.

But there is a negative side to these mushrooming data banks—particularly those bearing the imprimatur of a governmental organization. Consider the disclosure in 1970 that United States Army intelligence units had been engaging in systematic surveillance of the lawful political activity of a number of groups and had been preparing "incident" reports and dossiers on individuals who engaged in legal protests. This monitoring not only embraced society's "crazies" but also included such nonviolent organizations as the National Association for the Advancement of Colored People (NAACP), the American Civil Liberties Union (ACLU), the Southern Christian Leadership Conference, and the Women Strike for Peace and allegedly covered newsmen, congressmen, and a former governor. As hearings before the United States Senate made clear, the military pursued this surveillance with such unrestrained fervor that in a few short years countless Americans fell under its scrutiny.

Not only is the Army's file building difficult *to justify*, but it apparently was undertaken without any appreciation that the creation and exposure of dossiers on politically active people might deter them from exercising their constitutional rights to assemble, speak freely, or petition the government. If we really take our constitutional guarantees *seriously*, we canont allow them to be debilitated by coercive data collection. Claims of efficiency, national security, or the war against crime must not be permitted to justify every demand for gathering personal information.

> If we have a dictatorship of dossiers and data banks rather than of hobnailed boots, it will not be any less of a dictatorship.

INCREASING DATA COLLECTION

Because the current fear of surveillance is conducive to developing a "record prison" mentality, it is not surprising that some people suggest that the seeds of a police state or a return to McCarthyism are in the atmosphere.

Governmental assurances that file building will not be used for repressive purposes are not enough. For many, George Orwell's *Nineteen Eighty-Four* is a state of mind; even the *appearance* of repression has the impact of reality, especially when apprehensions are buttressed by arrogance of power on the part of public officials.

The problem, of course, goes well beyond political surveillance and affects us all. We live in an information-based environment in which computer technology increasingly is becoming society's central nervous system. Ever since the federal government entered the taxation and social-welfare spheres, greater quantities of information have been sought from citizens. Moreover, in recent years access to governmental or private largess has depended upon a willingness to divulge personal data.

As recording processes have become cheaper and more efficient, information collection has intensified. A form of Parkinson's Law is operating—as capacity for information handling has increased, there is a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, motivates the collection of information pertaining to a large number of subjects. (See also the article by John Rumsey, M.D., on page 22.)

DEEPER PROBING

The availability of electronic data storage and retrieval has accelerated this pattern, as evidenced by the increased detail required by tax forms and the dramatic expansion in governmental, industrial, and academic questionnaires. Surely a national health insurance program would lead to the establishment of a medical data bank, which then would be tied to computers administering a variety of other social benefit programs—and perhaps to those of the Internal Revenue Service.

One consequence of the advent of increased computer activity certainly will be that many governmental and private information-gathering agencies will go beyond current levels of inquiry, probing into such subjects as personal associations, location and activity, and attitudes toward various institutions and persons. In the medical field this already is occurring in the form of the threat to the physician/patient privilege and the practitioners privacy posed by the cost-justification demands of health insurers and the emerging professional service review programs.

Many risks lurk in this spiraling collection of data. As information accumulates, the contents of an individual's dossier tend to appear more and more impressive, despite the "softness" and dubious accuracy of much of it. The file imparts a heightened sense of reliability to the user, which, coupled with the myth of computer infallibility, makes it less likely that an independent evaluation of the subject will be made or that the data will be verified.

Blind faith in the written word is not a phenomenon unique to computerization. I know a talented college graduate who, unable to gain employment for a considerable period of time, learned that potential employers had been deterred by an entry in the file that her university had provided interviewers: "Melinda's mother is emotionally unstable." This notation had been made years before by a sixth-grade teacher, who was neither a psychiatrist nor a psychologist and had met the child's mother only casually. Yet this damaging comment was preserved and travelled with Melinda's academic dossier for 15 years without anyone bothering to question it or think about the propriety of disseminating it.

CONTEXTUAL ACCURACY

Not surprisingly, therefore, many people feel that their success or failure in life ultimately may turn on what other people put in their file and on an unknown programmer's ability—or inability—to evaluate, process, and interrelate that information. Insensitive computerniks and information users are as capable of injuring people by unintentionally rendering a record inaccurate, losing it, or mindlessly disseminating its contents as are those acting out of malice or for personal aggrandizement. Moreover, a computerized file has a certain indelible quality—adversities cannot be overcome with time, unless we develop an electronic eraser and a compassionate soul willing to use it.

The centralization of information from widely divergent sources also creates serious risks of using data out of context. The problem of contextual accuracy is best illustrated by one of the most dangerous types of personal information currently maintained—the unexplained, and often incomplete, arrest record. Consider the potential effect of this computer entry: "arrested, criminal trespass; sentenced, six months." Without more, how will a user—perhaps an employer or a credit grantor—know that this computerized "criminal" was, in reality, found "guilty" of demonstrating for desegregation in the South in the 1950s or for equal employment opportunities in the North in the 1960s under a state statute that was invalidated on appeal, and the conviction overturned as an unconstitutional restraint on free speech and assembly? Is it likely that the file subject's application will receive favorable treatment given this "record"? To make matters worse, it must be remembered that only a small number of those arrested are prosecuted and only a fraction of those prosecuted are convicted. Yet all will have arrest records—many of which will not even indicate the failure to prosecute or the acquittal!

And these records *will* circulate. Given the datamania in our society, information about people is valuable, especially if it is derogatory. Credit grantors, employers, detective agencies, insurance companies, political operators, and government investigators will pay for it or, on occasion, steal it.

The cavalier dissemination of personal information is encouraged by an informal "information buddy system." It is a striking fact that many bank and corporate security officers, private detectives, and field investigators for consumer-reporting companies are former federal or local law enforcement agents. The result is a subterranean dossier exchange network we can never confront that thrives on mutual backscratching or economic incentives.

What then is the solution? As an initial matter, one would hope that good judgment and self-regulation on the part of information gatherers and users would suffice. In that connection, let me offer five principles that are fundamental to the preservation of privacy against the anesthetizing effect of wide-scale computer use.

> A national health insurance program would . . . be tied to computers administering a variety of other social benefit programs—and perhaps to those of the Internal Revenue Service.

The first is a moral precept. Those who handle individualized data—whether it be financial profiles, student records, medical files, criminal records, welfare lists, or employment data—have an obligation to guard the privacy of the human beings whose lives are reflected in those dossiers and ensure that they are accurate and that only proper use is made of them.

Certain information should not be recorded. Without a compelling showing that the preservation of sensitive or highly personalized information, such as surveillance information on those pursuing lawful political and social activities, is essential to an important public policy, the recorder's hand should be stayed and the data permitted to be lost to man's memory or simply retained on a decentralized, unautomated, and highly confidential basis.

Access to data must be limited. Personal files should be available only to a restricted class of people whose access is authorized only after a careful examination of their need to know. This is particularly important in any system containing data from multiple sources, such as a hospital, a consortium of doctors, or a multistate mental health information center.

Accordingly, a wide range of technical, administrative, and procedural protections must be imposed on all personal-data systems. For example, anyone seeking access to an individual file must be required to identify himself, his dealings with the file recorded, and these records audited periodically. When information is transmitted into or out of a computer by telephone lines or microwave relays, it must be protected against wiretapping or other forms of electronic eavesdropping.

To improve the accuracy of computerized files and to give citizens some control over the information circulating about them, individuals should have access to dossiers pertaining to them and an opportunity to challenge their accuracy. The right to be protected against the dissemination of misinformation cannot be left to the winds of chance. This principle has been recognized in the Federal Fair Credit Reporting Act, which is the first step toward eliminating some of the abuses that result from the buying and selling of personal information by consumer-reporting companies.

Finally, personal information must not be allowed to petrify. Data that have become inaccurate, archaic, or of little probative value with the passage of time should be purged. Otherwise, the notion of redemption will be nothing but an illusion.

Despite self-restraint, however, Congress ultimately will have to strike the balance between effective exploitation of the new information technology and preservation of personal privacy. President Nixon's announcement in February, 1974, of the establishment of a top-level committee headed by Vice-President Ford to safeguard citizens' privacy is a promising omen.

One desirable legislative approach would be to prohibit governmental, and perhaps even nongovernmental, organizations from collecting certain types of data when there is no clear social justification for doing so.

The burden for maintaining the integrity of personal information could, of course, be placed upon computer manufacturers, users, and data networks. This somewhat different solution involves imposing a statutory duty of care on information handlers and promulgating comprehensive privacy and security regulations. Enforcement could be delegated to an information agency having the power to redress grievances and to conduct inquiries to determine whether the congressionally established code of conduct was being honored.

But beyond legislation, each of us must begin to counteract the syndrome referred to by the poet e. e. cummings when he wrote that "progress is a comfortable disease." We must overcome our complacent attitude toward the management of our affairs by what frequently are astigmatic administrators in both the government and the private sector.

The very real benefits conferred by information technology must not obscure the price being exacted in terms of personal freedom. The computer is precipitating a realignment in the pattern of societal power and is becoming an increasingly important decision-making tool for practically all significant governmental and non-governmetnal institutions. Thus, the central issue challenging us is how to contain the excesses and channel the benefits of this technological power.

If the concept and the preservation of personal privacy are fundamental to our tradition of individual autonomy, then the development of greater sensitivity to the danger of information abuse is imperative. Otherwise, we might awaken from our apathy someday to discover that the mantle of policymaking is being worn by specially trained technicians who have found the time to master the machine and are manipulating it for their own purposes. If we then have a dictatorship of dossiers and data banks rather than of hobnailed boots, it will not be any less a dictatorship.

[From the Congressional Record, Extensions of Remarks, Apr. 22, 1974]

THE RIGHT OF PRIVACY

Mr. ARCHER. Mr. Speaker, a combination of expanding computer technology and the growing power of the Federal Government has posed a threat to one of the most basic liberties of free people—the right of privacy.

An increasing involvement of the National Government in almost every aspect of an individual's life has led to an enormous collection of data gathered by a multiplicity of Federal agencies. It has been estimated that the U.S. Government has the capacity to secure about 20 pages of information on almost every man or woman in this country within 30 seconds by feeding a social security number into a data bank. In the hands of powerful bureaucrats, this information reported by a computer can be utilized in such a way as to invade the private lives of millions of Americans.

The effects of "Big Brother" government utilizing science and technology as a means of control have been portrayed in works like Aldous Huxley's "Brave New World" and "Brave New World Revisited," and George Orwell's "Nineteen Eighty-Four." Orwell described a vast records department, a branch of the Government's Ministry of Truth, which contained "every conceivable kind of

information, instruction, or entertainment, from a statue to a slogan, from a lyric poem to a biological treatise, and from a child's spelling book to a Newspeak dictionary." Many of the dangers to individual privacy contained in these fictional works appear to be reaching a reality in our own day.

Information fed into a data bank can reach enormous proportions when it is handled by the Federal Government. The Internal Revenue Service, the Federal Housing Administration, and the Social Security Administration are only a handful of Government agencies possessing extensive information on millions and millions of Americans. It is of great concern how rapidly this material can be disseminated throughout the Government to provide a complete profile on an individual.

Recently, this concern was expressed over the announced intention of the Department of Agriculture to look into the income tax returns of farmers as part of its statistic gathering operations. Fortunately, this permission was revoked by the President.

A prominent assistant professor in the field of urban studies at a leading midwestern university, critical of the accuracy of census data, proposed a system of permanent registration for everyone in the United States. This proposed permanent registration system would begin at birth and would include periodically cross-matching social security numbers with data obtained from birth and school records, the Internal Revenue Service, and other Federal and State statistical sources.

If adopted, this system would reduce each person to a mere number of statistic with the Government maintaining an up-to-date file on everyone in the United States. The justification for this type of information system would be easier to imagine in a totalitarian society; it is difficult to justify for a nation based on the right of individual freedom and privacy. Our Nation would be establishing its own records department so aptly described in Orwell's "Nineteen Eighty-Four."

If we are to maintain the rights of individuals in our society, we need to be especially cognizant of the right of privacy or the right to be left alone as an essential element in a free and democratic society. Realizing that everyday operations of government—local, State, and Federal—require the disclosure of some material facts, there must be a careful balance to preserve the individual's right to privacy by recognizing that he should be able to decide for himself when, how, and to what extent his attitudes, beliefs, behavior, and opinions should be disclosed to others. He should also have the right to exercise certain controls over the disclosure and nondisclosure of information to other people. It is unfortunate for freedom and dangerous to individual liberties that in the whole cycle of information collection and dissemination, the people most directly involved are excluded from the decision-making process. Justice Brandeis put it very effectively in Olmstead against United States:

"They (the makers of our Constitution) sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man."

It is encouraging that the President has established a Domestic Council Committee on Privacy, headed by the Vice President, which has as its task the examination of the whole range of data collection and to recommend actions which would provide each American a personal shield to protect his right to privacy. This concern for privacy has cut across party lines with the introduction of a great number of bills in the Congress to protect the various abuses of the right to privacy.

We should give priority consideration to legislation like H.R. 11276 which would prohibit the use of an individual's social security number or related record without his consent unless it is specifically required by law. This legislation would guarantee that an individual's social security number could only be used for matters directly related to the operation of old age, survivors and disability insurance programs. Restrictions on the use of the social security number will prevent the individual from becoming a mere number or statistic in government records and prevent government from obtaining unnecessary information from private companies and other government agencies on an individual for a massive goverment file. This bill would be an important step in the direction of preserving individual privacy.

It is essential that we act to preserve the right of privacy by making ourselves aware of the problem and adopting proper safeguards.

AMERICAN RIGHT OF PRIVACY

Address by the President

THE WHITE HOUSE, FEBRUARY 23, 1974

Over the years, historians and philosophers have continually debated about the roots of American greatness. There are almost as many theories as there have been scholars, but a single theme recurs again and again. It is the theme of individual dignity and individual rights—an ideal that permeates the Constitution's Bill of Rights and has been a fundamental part of American life since the founding of our Nation.

Generation after generation, we find America's best minds and greatest leaders emphasizing the need to protect the rights of the individual. In the Federalist Papers, James Madison said that the twin duties of enlightened government were "to secure the public good" and to secure "private rights." In our own time, President Eisenhower reaffirmed that ideal. He said, "The supreme belief of our society is in the dignity and freedom of the individual."

In James Madison's day, the American Revolution was fought to establish a new nation based on this principle. By the time Dwight Eisenhower was President, America had passed through a tragic Civil War and two bloody World Wars fought in defense of the same principle. But it is not on the battlefield alone that individual liberties are threatened and must be defended.

In peace as well as in war, social, economic, political and technological forces are constantly at work that can either help or hinder the individual American's quest for "life, liberty and the pursuit of happiness."

Many things are necessary to lead a full, free life—good health, economic and educational opportunity, and a fair break in the marketplace, to name a few. But none of these is more important than the most basic of all individual rights, the right to privacy. A system that fails to respect its citizens' right to privacy, fails to respect the citizens themselves.

There are, of course, many facts which modern government must know in order to function. As a result, a vast store of personal data has been built up over the years. With the advent of the computer in the 1960's, this data gathering process has become a big business in the United States—over $20 billion a year—and the names of over 150 million Americans are now in computer banks scattered across the country.

At no time in the past has our Government known so much about so many of its individual citizens. This new knowledge brings with it an awesome potential for harm as well as good—and an equally awesome responsibility on those who have that knowledge.

Though well intentioned, Government bureaucracies seem to thrive on collecting additional information. That information is now stored in over 7,000 Government computers. Collection of new information will always be necessary. But there must also be reasonable limits on what is collected and how it is used.

The same process has been at work in the private sector where computers and modern data technology have placed vast quantities of personal information in the hands of bankers, employers, charitable organizations and credit agencies.

On the positive side, the availability of this information serves us all in many important ways.

Without computer technology, it would, for example, be extremely difficult to process and deliver 27 million Social Security checks every month, to send out veterans benefits, and to ensure that Medicare payments are properly made.

Law enforcenment agencies would not and could not combat new and sophisticated criminal activities without the use of the latest technical developments in the data field, whether in helping to trace stolen goods, or in helping to track down and identify criminals.

In the private sector, the banking industry could not even start to cope with the vast volume of personal checks which are issued and cashed daily without using computer technology.

No modern industrial society can survive without computers and data processing—and especially a society with high living standards and even higher expectations such as ours.

Many of the good things in life that Americans take for granted would be impossible, or impossibly high-priced, without data retrieval systems and computer technology. But until the day comes when science finds a way of installing a conscience in every computer, we must develop human, personal safeguards that prevent computers from becoming huge, mechanical, impersonal robots that deprive us of our essential liberties.

Here is the heart of the matter: What a person earns, what he owes, what he gives to his church or to his charity is his own personal business and should not be spread around without his consent. When personal information is given or obtained for one purpose such as a loan or credit at a store, it should not be secretly used by anyone for any other purpose.

To use James Madison's terms, in pursuing the overall public good, we must make sure that we also protect the individual's private rights.

There is ample evidence that at the present time this is not being adequately done. In too many cases unrestricted or improper use of personal information is being made.

In some instances, the information itself is inaccurate and has resulted in the withholding of credit or jobs from deserving individuals. In other cases, obsolete information has been used, such as arrest records which have not been updated to show that the charges made against an individual were subsequently dropped or the person found innocent. In many cases, the citizen is not even aware of what information is held on record, and if he wants to find out, he either has nowhere to turn or else he does not know where to turn.

Whether such information is provided and used by the Government or the private sector, the injury to the individual is the same. His right to privacy has been seriously damaged. So we find this happens sometimes beyond the point of repair. Frequently, the side effect is financial damage, but it sometimes goes further. Careers have been ruined, marriages have been wrecked, reputations built up over a lifetime have been destroyed by the misuse or abuse of data technology in both private and public hands.

It is clear, as one Government study has concluded, that "it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems." Fortunately more and more people are becoming aware of this growing threat.

The Fair Credit Reporting Act of 1970 which I signed into law took a major first step toward protecting the victims of erroneous or outdated information. It requires that an individual be notified when any adverse action, such as denial of credit, insurance or employment, is taken on the basis of a report from consumer-reporting agencies. It also provides citizens with a method of correcting these reports when they contain erroneous information.

Many public and private statistical organizations which collect personal data have shown an awareness of their own responsibility to prevent unfair disclosure and to eliminate inaccurate or obsolete information.

Earlier this month, Attorney General Saxbe proposed legislation to the Congress which would establish rules governing the collection and use of criminal justice information, and the Congress itself has conducted extensive hearings into the uses and the abuses of data banks, credit bureaus, and personal records.

All of this is action in the right direction, but we must go further and we must move quickly.

What was once a minor problem affecting only a small number of people has now become a national problem that could potentially affect every American with a charge account, a service or personnel record, a credit card, a Social Security number, a mortgage, or an appliance or automobile bought on time. In short, data banks affect nearly every man, woman and child in the United States today.

To meet a challenge of these dimensions, we need more than just another investigation and just another series of reports. We need action. That is why I am today establishing in the White House a top priority Domestic Council Committee on the Right of Privacy. This will not just be another research group. It will be a panel of some of the most able men and women in the Government, and it will be primed for high-level action.

It will be chaired by Vice President Ford, it will include the Attorney General and five other Cabinet members—the Secretaries of the Treasury, Defense, Com-

37-583 O - 74 - pt. 2 - 32

merce, Labor, and Health, Education, and Welfare—along with the Chairman of the Civil Service Commission, the Director of the Office of Management and Budget, the Director of the Office of Consumer Affairs, and the Director of the Office of Telecommunications Policy.

This is no ordinary group, and the task I have set for it is no ordinary task.

This Privacy Committee will build on the fine work that other groups have already carried out, and I will see to it that it is supported by the best talent available in determining the views of representatives from the legislative branch, the judicial branch and the private sector, including our colleges and universities.

I am asking the members to examine three key areas of concern: collection, storage and use of personal data. Specifically, the committee will examine:

—How the Federal Government collects information on people and how that information is protected;

—Procedures which would permit citizens to inspect and correct information held by public or private organizations;

—Regulations of the use and dissemination of mailing lists;

—And most importantly, ways that we can safeguard personal information against improper alteration or disclosure.

All of this will require extensive work by the Committee, but it is only the first half of the job.

Once the information and views of all parties concerned have been thoroughly aired, the Committee will be responsible for developing a comprehensive series of specific recommendations for action. I want that action to provide a personal shield for every American which he can use to protect his right to privacy.

I am directing this blue-ribbon panel, within four months, to begin providing a series of direct, enforceable measures—including regulations, executive actions, policy changes, legislation where necessary and voluntary restraints—all of which we can immediately begin to put into effect.

Advanced technology has created new opportunities for America as a nation, but it has also created the possibility for new abuses of the individual American citizen. Adequate safeguards must always stand watch so that man remains the master—and never becomes the victim—of the computer.

In the first half of this century, Mr. Justice Brandeis called privacy the "right most valued by civilized men." In the last half of this century, we must also make it the right that is most protected.

Thank you and good afternoon.

FACT SHEET ON THE PRESIDENT'S ADDRESS ON THE AMERICAN RIGHT OF PRIVACY OF FEB. 23, 1974

BACKGROUND

In his State of the Union Address to the Congress on January 30, 1974, the President stated his intent to "make an historic beginning on the task of defending and protecting the right of personal privacy for every American". In today's address, the President announced that he had ordered an "extensive Cabinet-level review" to determine what measures can be taken to assure personal privacy while meeting legitimate needs for information. Today's address further defines the nature of the problem, announces the composition of the Committee, and outlines action to be taken.

INITIATIVES ANNOUNCED TODAY

Establishment of a Domestic Council Committee on the Right of Privacy

The Domestic Council Committee which the President is announcing today will consist of: The Vice President, Chairman; Secretary of the Treasury, Secretary of Defense, Attorney General, Secretary of Commerce, Secretary of Labor, Secretary of HEW, Chairman, Civil Service Commission, Director, Office of Management and Budget, Director, Office of Telecommunications Policy, and Director, Office of Consumer Affairs.

The Committee will be supported by a staff comprised of personnel paid by the principal agencies concerned; headed by an Executive Director soon to be designated.

It is also anticipated that advisory committees and consultants will be employed to provide special expertise which the Committee may need and to ensure the full presentation of differing points of view.

An agenda for action

The President, in his address today, indicated that he expects the Committee to review government and industry practices and recommend specific measures which can be taken to ensure that the individual's right to privacy is protected. Specific areas which the Committee is being asked to address include:

—Trafficking in records containing identifiable personal information. Much of the information about individuals is assembled and processed by third parties in government and private industry, whom the citizen has little knowledge and control of, even though it is the individual who could be adversely affected by wider dissemination of the information. Can we improve the method of regulating the activities of those who assemble, process, and disseminate such information?

—Relevance and adequacy of consent to disclose personal information. Although many people consent to the gathering of information about themselves, they often do so only when important benefits, such as receiving credit, insurance, financial assistance, government benefits or even jobs, are conditioned on the disclosure of sensitive information. One goal of privacy protection is to assure that undue advantage is not taken when people are dependent on such benefits. More attention should be directed at the privacy rights of welfare recipients, medicare patients, and others participating in Federally-funded health, educational and welfare programs.

—Do we leave too many final decisions on the nature and type of information to be collected to government and private officials who have no particular

interest in minimizing the information to be sought? Can we place such officials in a position of answering whether the benefit of having personal information outweights the intrusion upon individual privacy of obtaining it? Do we need new organizations or methods to assure that privacy concerns are reflected and accommodated in government and private programs? There may be a need for a code of fair record keeping practices for both the public and private sectors. The Committee will consider the most appropriate means for promulgating necessary policies and assuring their consistent implementation.

—Lessening the amount of information that is acquired and collected. Information that is not collected cannot be used to abuse. If computerized files are replete with unnecessary and irrelevant information, it may not be sufficient that the individual has the ability to inspect and correct records and control their further dissemination. Should there be a requirement that, when asked to supply personal data, the individual should be informed of whether he is legally required to provide such data, of any specific consequences of providing or not providing the data; should he be able to test the need or authority to request the data?

—Knowledge of information, collection; use and dissemination activities. Solutions to privacy abuses that have arisen may lie in the area of increasing the individual's ability to find out what information about him is being collected or is in a record and how it is used; to correct or amend an inaccurate or incomplete record; and to prevent information about him obtained for one purpose from being used or made available for another purpose. Government and private organizations maintaining records of identifiable personal data may be required to adopt strict data security and access rules, as well as physical safeguards to protect the data. Should they also be required to assure the reliability of the data for their intended use and must they take precautions to prevent its misuse?

—Additional enforcement mechanisms. How can government and private industry adopt meaningful ways to enforce general principles and broad safeguards regarding privacy, and adopt legal, administrative, and voluntary remedies.

—The adequacy of present laws regarding credit reporting practices and the secrecy of bank records. Experience under existing legislation concerning fair credit reporting and the secrecy of bank records should be analyzed to determine whether additional enforcement mechanisms are necessary.

—Conflicts with interests protected by the Freedom of Information Act. There may be a number of instances in which the privacy and security of Government-held personal information records conflict with the public interest principles reflected in the Freedom of Information Act; any such conflicts will be explored.

—The relationship of state and local information systems to Federal systems. There should be a thorough review of Federal assistance practices with respect to state and local data systems which could have the effect of absorbing such systems into nationwide, Federally-controlled communications and computer information systems.

—Survey of personal investigation and reporting activities. There may be a need to determine precisely which entities and organizations in government and in private industry conduct or extensively reply upon investigative reports on individuals.

—Federal personal record keeping practices. The Federal Personal Manual, issued by the Civil Service Commission prescribes certain record keeping policies for civilian employee records including the individuals right to inspect certain records. The Department of Defense has similar regulations for military records. The Committee will examine the appropriatness and adequacy of these policies.

—Regulations governing the personal record keeping practices of Federal contractors and grantees. The Committee will review the need and authority for rules and regulations to assure that Federal contractors and grantees are adequately safeguarding personal data.

—Appropriate non-criminal justice uses of criminal offender record information. This question has arisen in connection with the proposed Criminal Justice Information Act, cited above.

—Limiting the use of the Social Security Number as a standard personal identifier. In the absence of other adequate safeguards it has been suggested

that policies be adopted to make it as difficult as possible to link and compile personal data from various sources.

—Possible regulation of the use and dissemination of mailing lists. The propriety of constructing name and address lists from personal information collected for other purposes has been questioned.

—The development of techniques and procedures to safeguard personnel records against improper modification or disclosure. This may be viewed as the security dimension of the privacy issue. The Committee will examine the adequacy of existing measures for making personal data as safe as possible by limiting the number of individuals who can access it, preventing improper or inadvertent modification of data, and other measures.

—An evaluation of other government's experience in licensing personal data systems. The Swedish privacy law calls for the licensing of such systems and the 1972 British Report of the Committee on Privacy (The Younger Report) recommended that consideration be given to this approach.

—Appropriate safeguards for statistical and research systems which are based on aggregations of personal data. Both the HEW Advisory Committee Report and the 1971 Report of the President's Commission on Federal Statistics suggest possible means for strengthening protection of individual records.

—Because of the Congressionally created National Commission for Review of Federal and State Wiretapping Laws, the President asked that his own Domestic Council Committee on Privacy defer recommendations in this area pending receipt of the Wiretap Commission's Report.

Executive—Legislative development

A great deal of activity and information collection has already occurred in the privacy area. This includes the landmark legislation regulating private credit rating companies (The Fair Credit Reporting Act of 1970), the development of safeguards for a substantial amount of the statistical information collected by the government, and an extensive study by HEW on Automated Personal Data Systems. The Department of Justice has recently submitted proposed legislation regulating the exchange and dissemination of criminal justice information.

The Fair Credit Reporting Act of 1970 (Title VI, PL 91-508)

The purpose of this legislation is to assure that individuals are not unfairly denied credit or employment as a result of erroneous data.

—The Act gives consumers access to information (except medical information) in their credit files and enables them to correct inaccurate or misleading information.

—Should a person be turned down for credit, insurance or employment because of an adverse credit report, he must be so advised and given the name and address of the credit reporting agency.

—Credit agencies are required to delete any inaccurate or unverifiable information.

—The Act assigns administrative enforcement authority to the Federal Trade Commission, except in banking and other specific areas where other Federal regulatory agencies have supervisory authority. Consumers can bring civil actions to recover any actual damages sustained as a result of ordinary negligence by credit reporting agencies. Consumers are also permitted to collect punitive damages for willful noncompliance by consumer reporting agencies.

Safeguards for statistical information

The statistical community, both public and private, has a long tradition of protection of the confidentiality of personal and business information. Their successes can provide valuable guidelines to extend further the protection of individual privacy. This is illustrated by the evolution of procedures for census data.

—Until the 1880 Census, copies of census schedules were immediately available to the public in courthouses. For the 1880 Census, a statutory provision was enacted which required enumerators to swear that they would not disclose "any information on the schedules" to anyone other than their superior officers.

—For the 1900 Census, the disclosure provision was extended to cover all employees of the Census Office. This provision is still in force.

—In 1952, because the decennial population censuses are a unique source of detailed demographic data, individual records of the 1880 Census were made available to researchers.
—In 1973, the 1900 Census records were made aavilable by the Archivist to persons engaged in "legitimate historical, legal, genealogical or other worthwhile research."

There are many current policies to preclude disclosure of individually identifiable data collected for statistical purposes.

—Under Title 13 USC no Census employee may use Census information for any purpose other than statistical purposes, published data whereby any establishment or individual can be identified, or permit any other than sworn employees of the Commerce Department to examine the individual reports. Any employee who communicates any information without written authority can be fined up to $1,000 or imprisoned for two years or both.
—Labor Department regulations admonish the Commissioner of Labor Statistics to protect the confidentiality of data collected by BLS and assigns him responsibility for ensuring that data collected for BLS by other organizations is obtained under adequate guarantees of confidentiality.
—Public Health Service has long collected vital statistics under specialized and stringent guarantees of the confidentiality of individual records.
—By law, the Social Security Administration is not permitted to disclose any information about individuals except as provided by the Secretary of Health, Education, and Welfare. Exceptions have been generally limited to checking of income (where income is a condition of eligibility for an income maintenance program), release of information to Federal or State employees administering unemployment insurance, and a limited number of research projects.

The HEW Secretary's Advisory Committee on Automated Personal Data Systems

In July 1973, a committee of prominent individuals from State and local governments, industry and academia submitted its report on *Records, Computers and the Right of Citizens** to the Secretary of Health, Education, and Welfare. The report has served to define many of the questions involved in protecting personal privacy.

The report recommends the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems. The code would be built around five "principles of fair record keeping practices".

—There must be no personal data record keeping system whose very existence is secret.
—There must be a way for an individual to find out what information about him is in a record and how it is used.
—There must be a way for an individual to prevent information about him that was obtained for one purpose from being used for other purposes without his consent.
—There must be a way for an individual to correct or amend a record of identifiable information about him.
—Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data."

The report recommends adoption of added safeguards for administrative personal data systems based on the following five principles.

—"When personal data are collected for administrative purposes, individuals should under no circumstances be coerced into providing additional personal data that are to be used exclusively for statistical reporting and research. When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's responses should be made clear.
—Personal data used for making determinations about an individual's character, qualifications, rights, benefits, or opportunities, and personal data collected and used for statistical reporting and research, should be processed and stored separately.

---

*The report is available for sale by the Superintendent of Documents, Stock No. 1700-00116.

—The amount of supplementary statistical-reporting and research data collected and stored in personally identifiable form should be kept to a minimum.
—Proposals to use administrative records for statistical reporting and research should be subjected to careful scrutiny by persons of strong statistical and research competence.
—Any published findings or reports that result from secondary statistical-reporting and research uses of administrative personal data systems should meet the highest standards of error measurement and documentation."

The report recommends against adoption of *any* standard identifier for individuals and recommends limitations on the use of the Social Security Number.

—"Uses of the SSN should be limited to those necessary for carrying out requirements imposed by the Federal Government.
—Federal agencies and departments should not require or promote use of the SSN except to the extent that they have a specific legislative mandate from the Congress to do so.
—The Congress should be sparing in mandating use of the SSN, and should do so only after full and careful consideration preceded by well advertised hearings that elicit substantial public participation. Such consideration should weigh carefully the pros and cons of any proposed use, and should pay particular attention to whether effective safeguards have been applied to automated personal data systems that would be affected by the proposed use of the SSN."

The Criminal Justice Information Systems Act of 1974

The Attorney General has submitted proposed legislation (introduced as S. 2964/H.R. 12574) to facilitate and regulate the exchange of criminal justice information in order to insure the security of criminal justice information systems and to protect the privacy of individuals to whom the information in such systems pertains.

The bill divides criminal justice information into three categories:

—Criminal justice intelligence information, including investigative files and other such "subjective information."
—Criminal offender processing information, including medical and other reports on individuals in the correctional system,
—Criminal offender record information, including mainly information such as arrest and disposition records, probation status, and physical identification data.

The bill would restrict direct access to criminal justice information to officers or employees of criminal justice agencies and permit all three categories of information to be used for criminal justice purposes. It also defines the circumstances under which the information may be used for noncriminal justice purposes.

—Criminal intelligence information may be made available (a) when determined by the Attorney General to be necessary for reasons of national defense or foreign policy, and (b) when compiled by a criminal justice component of a noncriminal justice agency and used by the same agency for statutory functions.
—Criminal offender processing information may be made available (a) to the individual concerned when authorized by court order or Federal or State statute or regulation, (b) for research pursuant to the Attorney General regulations, (c) for research related to criminal justice, and (d) for other use as authorized by court or Federal or State statute.
—Criminal offender record information may be made available (a) to the individual to whom information pertains (b) for research related to criminal justice, and (c) for other purposes expressly provided for by Federal statute.

In addition, the bill—

—Affords an individual access to his offender record information for purposes of correcting his record.
—Requires the individual about whom offender record information is requested for a non-criminal justice purpose to be notified by the requester that such information about him is being sought.

—Requires scaling of an individual's criminal offender record information after a specified period with a clear record, either five or seven years, depending on the nature of the conviction.
—Requires arrest data release for a non-criminal justice purpose to include final disposition, if known, and prohibits release of arrest data for such purpose if the charge resulted in acquittal, or was dismissed or not disposed of within a year.
—Places responsibility for the accuracy and up-dating or criminal offender record information on the agency initially contributing the information to the system.
—Establishes administrative, civil and criminal sanctions against those who use or disseminate information in violation of the Act.

CONGRESSIONAL ACTIVITIES

The Congress has conducted a number of inquiries into record keeping practices and their effects on personal privacy. These inquiries have helped to define the issues which must be addressed. These include:

Year	Committee	Subject of inquiry
1965	Senate, Judiciary	Invasions of privacy.
1965	do	Psychological tests and constitutional rights.
1965	House, Government Operations	Invasions of privacy
1966	House, Post Office, and Civil Service	Census questions.
1966	House, Government Operations	Computers and the invasion of privacy.
1967	Senate, Judiciary	Computers and privacy.
1967	do	Rights of Privacy Act of 1967.
1967	House, Post Office, and Civil Service	Questions in the census.
1967	Joint Economic Committee	Coordination and integration of Government statistica programs.
1969	House, Post Office, and Civil Service	1970 census legislation.
1969	Senate, Judiciary	Privacy, the census and Federal questionnaire.
1971	House, Government Operations	Federal personnel records.
1971	Senate, Judiciary	Federal data banks, computers and Bill of Rights.

Currently:
—The House Committee on Government Operations is conducting hearings into the need for legislation governing Federal Personal record keeping.
—The House Judiciary Committee is considering the Criminal Justice Information Systems Act of 1974.
—The Senate Judiciary Committee is completing a survey of Federal data banks which contain personal data about individuals.

National Commission for Review of Federal and State Wiretapping Laws

The Commission was established by Title III of the Omnibus Crime and Safe Streets Act to conduct a comprehensive study and review of the operation of the provisions of Title III, regarding wiretapping and electronic surveillance, in order to determine their effectiveness during the six-year period following June 19, 1968.

The Commission is to be composed of 15 members appointed as follows:
—Four appointed by the President of the Senate from members of the Senate; members are: John L. McClellan, James Abourezk, Roman L. Hruska, and Robert Taft, Jr.
—Four appointed by the Speaker of the House from members of the House, no extant appointments, previous appointments have lapsed;
—Seven appointed by the President from various walks of life, none of whom shall be officers of the executive branch; members are: Richard W. Anderson—Omaha Police Chief; G. Robert Blakey—Cornell Law Professor; Samuel R. Pierce, Jr.—former Treasury Counsel; Florence P. Shientag—Attorney; Alan F. Westin—Columbia University Professor; Frank J. Remington—Wisconsin Law Professor; and William H. Erickson—Colorado Supreme Court Justice.

The Chairman of the Commission, appointed b ythe President, is William H. Erickson.

The Commission, a designated subcommittee, or member thereof, may hold such hearings as is deemed necessary to carry out the Commission's function. The Commission is granted the power to subpoena witnesses, books, records,

documents, etc., to be issued by the Chairman, or designated member of the Commission. The Chairman may enforce such subpoenas through the U.S. District Courts. Each department or agency of the executive branch of government, including independent agencies, is authorized and directed to furnish such data as the Commission requires to fulfill its functions upon the request of the Chairman. The Chairman is also authorized to seek relevant data and information from the appropriate offices of the several States.

$332,000 has been appropriated for fiscal year 1974 to carry out the provisions of the authorizing section, and $500,000 has been requested for fiscal year 1975.

SURVEY OF GOVERNORS AND STATE ATTORNEYS GENERAL ON S. 3418, PRIVACY, AND STATE LAWS

STATE OF ALABAMA

AUGUST 16, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: Thank you for your letter of June 25, 1974, in which you invited me to give my opinion concerning S. 3418. I appreciate very much the opportunity to submit my views on this important bill.

In answer to the question contained in your letter, I would like to inform you that no action is currently being taken on the State or local level in Alabama on privacy matters or issues.

I commend you, Senators Percy and Muskie, and the other members of Congress who are concerned about dangers to privacy and who are acting to protect the citizens of the United States in this vital and urgent area. Your concern is one which I share and it is particularly timely because of Watergate, as you pointed out on the floor of the Senate on May 1, 1974. However, there is at least one aspect of S. 3418 which I do not favor.

Many forms of crime represent the ultimate intrusion into privacy. Crime not only chills the exercise of precious rights but also destroys life and property as well as emotional well-being. It is a problem of alarming proportions and one which affects every American. Because of this, any legislative effort to protect privacy which makes it more difficult for law enforcement agencies to solve crimes and apprehend criminals raises difficult public policy questions.

The importance of ensuring individual rights of privacy and the need to wage an effective battle against crime pose a serious and complex problem. It is my opinion that this serious and complex problem deserves the individual consideration and treatment of special legislation. General privacy legislation is too blunt a tool for it, and both privacy and effective law enforcement can lose as a result. As merely one example consider the application of S. 3418 on the National Criminal Information Center system.

As a result of six years experience as a District Attorney and four years experience as an Attorney General, I am convinced that the N.C.I.C is one of the most effective tools law enforcement has. Because the N.C.I.C. helps solve crimes and apprehend criminals it saves countless lives and millions of dollars in property each year.

No provision of S. 3418 exempts the N.C.I.C. from the application of it. Section 202(2) seems to provide no exemption for the N.C.I.C. because of the "except" clause in it. Given the applicability of S. 3418, certain of its provisions at least suggest potentially crippling restraints on the N.C.I.C. For example, what will be the impact of Section 201(a)(2)? Will Section 201(d)(3)(B) jeopardize the security of informants?

Will Section 201(d)(3)(c) require disclosure of an investigation at a time when it is crucial to keep the fact of the invesigation secret? To consider a more specific and a timely example, note the possible impact of Section 201(a)(13) on criminal information files about such political terrorist groups as the Weathermen and the Symbionese Liberation Army. Can it be said with certainty that Section 201(a)(13) would permit a law enforcement agency to identify a criminal in N.C.I.C. or other files as a member of those two or other political terrorist groups? If not, then the bill will unnecessarily hinder the identification and apprehension of persons responsible for kidnappings, robberies, bombings, and other violent crimes.

What answers the courts will give to the questions pointed out above is less important at this stage than the fact that S. 3418 does not answer the questions itself. The fact such questions abound demonstrates that it is unwise to attempt to regulate in a general privacy bill the very important and complex privacy problems raised by criminal information systems. Regulation of such systems is urgently needed particularly in regard to access to criminal information files by agencies other than law enforcement. In fact, I think that regulation of criminal information systems is one of the most serious and urgent privacy problems our society faces, but the importance of the problem underscores the need for separate regulation.

Based on the reasons suggested above I respectfully suggest that S. 3418 clearly exempt criminal information systems and that separate legislation be prepared to regulate such systems.

Thank you again for the opportunity to submit my views on this matter. Please let me know if I can ever be of any assistance to you.

Sincerely,

BILL BAXLEY, *Attorney General.*

STATE OF ARKANSAS

OFFICE OF THE GOVERNOR,
LITTLE ROCK,
July 16, 1974.

Hon. SAM J. ERVIN, Jr.,
Senator U.S. Senate,
Washington, D.C.

DEAR SENATOR ERVIN: I was pleased to receive your letter of June 25 discussing S. 3418 together with the attached information. In my opinion this legislation is most timely, and its enaction into law in some form is critical to the well-being of the country.

We have witnessed over the last two decades a growing concern for and awareness of each individual's constitutionally protected right to privacy. It's almost as if this concern has grown in direct proportion to the proliferation of computers and data banks.

As a Governor, I know how necessary and sometimes how critical it is to have full and complete information on programs and personnel at one's fingertips. In Arkansas, for example, we are currently in the throes of establishing a computerized information system for state agencies for the express purpose of centralizing and expediting comprehensive data to assist the Governor and his Department Heads in making the complex decisions that are part of day to day state government.

On the surface, this computerized information system is devoutly to be wished, but I am also cognizant of the very real constitutional problems that can evolve if the system is not correctly administered. As a result, I have advised the Director of the program that safeguards must be built into the system (1) to limit the availability of information to specified persons; (2) to permit individuals to investigate data directly applicable to them; and (3) to provide individuals with procedures for the correction of erroneous data.

Arkansas government presently has several computers in operation, one of which is used for criminal justice and highway safety information. This system contains traffic violations and criminal history, although arrest warrants are purged after they are served so that only outstanding arrest warrants are included in the data bank. Moreover, we have establised procedures for our citizens to determine what information is contained on them in the data bank and to correct any errors.

Arkansas is not part of the NCIC program of the FBI because we have refused to dedicate a computer solely for criminal history purposes or to agree to the Bureau's regulations concerning the availability of this information.

I will watch the progress of S. 3418 with great interest, and I am taking the liberty of forwarding your information to the Administrator of our Criminal Justice-Highway Safety Information Center and to the State Attorney General, who is Chairman of this program for their additional comments.

Hopefully, I will be in Washington in time to have some input into this legislation. After all, 1984 is only ten years away.

Sincerely,

DALE BUMPERS.

STATE OF CALIFORNIA

OFFICE OF CRIMINAL JUSTICE PLANNING,
SACRAMENTO, CALIFORNIA,
July 22, 1974.

Hon. SAM J. ERVIN, Jr.,
U.S. Senate Committee on Governmental Operations,
Washington, D.C.

DEAR SENATOR ERVIN: Governor Ronald Reagan has asked me, as Executive Director of the California Office of Criminal Justice Planning, to respond to your recent letter soliciting comments on S. 3418. While we share your concern that confidential data on citizens remain confidential, there are several areas in which the bill could interfere with efforts being made to improve the criminal justice system in California.

I am enclosing copies of relevant portions of the California Penal Code.[1] As you will see, California has adopted some progressive measures which go beyond the limits of S. 3418, and is continuing to experiment with further measures in this area.

The provisions requiring a record of every access and the purpose for such access to our statewide criminal files, as required in Section 201(a)(9) of S. 3418, would be unduly burdensome. Since access to the information is already severely limited under California law, the provision would seem unnecessary to protect an individual's privacy. The increased cost involved would greatly detract from the efficiency and effectiveness of our statewide criminal justice information network.

In other areas, our existing California law does more to protect the privacy and security of confidential data, and is, in some respects, inconsistent with your bill. The bill presently would require, in Section 201(d)(5), that we must correct an individual's criminal record if the information is found to be incorrect. This is already part of California law, under Penal Code Section 11126. But California goes on to give an individual the right to an impartial fair hearing when the information is challenged. This goes beyond the provisions of S. 3418 that would require us to merely include the individual's version of the dispute when there is a conflict. Further, to include a 200 word contradictory "defendant's version" of every arrest or conviction in his criminal record could prove to be a major burden in that some criminal records could become extremely lengthy.

In Section 201(a)(4), the bill calls for maintaining information "with accuracy, completeness, timeliness, and pertinence". California again is showing its dedication to this goal by purging its files of data which is out of date and no longer relevant. This purge program, which is costing the state millions of dollars, will eliminate dated and unnecessary information in our criminal files.

The exemption for criminal investigation files in Section 202(2) of the bill is necessary, and ought to be expanded to include all criminal files authorized by state law. This would allow California to continue to experiment in this field and to go beyond the provisions of S. 3814 in guaranteeing privacy and security of personal data in our criminal information systems.

We appreciate the opportunity you have given us to work with you in developing legislation in this important field.

Sincerely yours,

ANTHONY L. PALUMBO,
Executive Director.

Attachments.

STATE OF CALIFORNIA,
OFFICE OF THE ATTORNEY GENERAL,
DEPARTMENT OF JUSTICE,
August 26, 1974.

Hon. SAM J. ERVIN, Jr.,
Senator, U.S. Senate, New Senate Office Building, Washington, D.C.

DEAR SENATOR ERVIN: Thank you for your letter of June 25, 1974, requesting our views concerning S. 3418, as well as information concerning action taken by the State of California on privacy matters.

For several years California has been working to control the use and dissemination of files maintained by local and state criminal justice agencies. Under

---

[1] See enclosures to California Department of Justice letter to Senator Ervin dated August 26, 1974, following.

California law criminal history information is disseminated only to agencies and individuals authorized by statute. At the present time the California Department of Justice is sponsoring legislation to make improper dissemination or receipt of criminal history information a crime. Under California law prompt and accurate reporting of criminal dispositions is required and the subject of a criminal history record is allowed the opportunity to review the record for inaccuracy or incompleteness and to have the record corrected if necessary.

Pursuant to law the California Department of Justice is given the responsibility of establishing statewide standards for the security and privacy of criminal history information. At the present time it is anticipated that regulations setting appropriate standards will be in effect in California in January of 1975. In addition, the California Department of Justice has instituted a policy of purging records which have lost their useful value because they are too old or deal with minor offenses. Enclosed for your informaton is an attachment which contains copies of the laws, proposed laws, and departmental policies which have been referred to above.

We believe that California leads the nation in developing the delicate balance between the need of the public to have an efficient criminal justice information system, and the need of the public to have their privacy and reputation protected from the improper or inadvisable use of criminal records.

The progress which California has made in the criminal records area, however, has not been matched by progress in correcting the problems which still exist in the area of private information systems. An attempt to impose controls over private information systems was made in Assembly Bill 2656 (copy enclosed) which was introduced during the 1973–74 session of the California Legislature. However, this proposal received strong opposition from private interests, and in its present form has been amended to apply only to governmental agencies.

In reviewing the provisions of S. 3418, we would like to offer general comments as well as specific criticisms.

We feel that the scope of S. 3418 is too broad. It attempts to cover every type of private or public information system which maintains personal data. It is inadvisable to attempt to control in the same proposal information systems maintained by private industry or businesses, non-criminal justice public agencies, and criminal justice agencies. Restrictions which are reasonable in one context may not be reasonable in the other.

For example, one of the essential needs of a criminal justice agency is confidentiality of the information which it maintains. This is not required because of the desire of law enforcement officials to subvert the civil rights of the people whom they serve, but rath reis necessary if law enforcement officials are to be able to effectively combat criminal activity. Often information contained in an investigatory file pertaining to, for example, an organized crime figure will disclose the names of informants, the extent of surveillance of the subject, and other information which if known to the subject would compromise the ability of the law enforcement agency to protect the public from his activities. On the other hand, confidentiality is not normally a needed feature of records maintained by private industry or non-criminal justice agency records. In fact, in many cases a major use of private or non-criminal justice public records is to sell the information contained in them to mailing houses or similar businesses.

This dichotomy is exemplified by the effect of the requirement in sections 201(d)(3) and (4) of S. 3418. These subdivisions would allow a person who is the subject of an information file to have access to a summary of the information in the file, to be told the nature of the sources of information in the file, to find out who is receiving the information in the file, and to personally review information in the file. The adverse impact of this provision upon an organized crime intelligence file is obvious. It would destroy the coinfidentiality of the file, thus reducing the ability and effectiveness of law enforcement in this area while encouraging the expansion of organized crime activity throughout the country. On the other hand, its impact upon a non-criminal justice agency or upon a private business would in most cases be mainly in terms of the cost and inconvenience of allowing the individual to have access to the information.

We also believe that legislation in this area should carefully distinguish between automated systems and manual systems. It is often rather easy to comply with security requirements in an automated system. In such a case, the system simply needs to be programmed to meet the contingencies contained in the security regulations or law. It is much more difficult and costly to comply with such restrictions in a manual system, and careful consideration should be given

to this fact when drafting legislation which applies to both manual and automated systems.

We are concerned that the standards outlined in S. 3418 are too narrowly drawn and impose standards which in many cases may be contrary to reasonable security and privacy efforts being made by the states. It is reasonable to establish a federal level board empowered to develop general guidelines to be followed by the states in protecting the security and privacy of individuals from manual and computerized information systems. We feel, however, that these guidelines should be broad enough to allow a diversity of approaches among the various states, and to allow the states to take into account their differing social conditions and privacy problems.

An example of the inadvisability of detailed federal controls in this area is seen in sections 201(a)(8) and (9) of S. 3418. Basically, these sections require an information system to maintain a list of persons having regular access to personal information in the system, as well as a complete list of the identity of persons using the system, and the purpose of every access to the system.

In a small state with a relatively small population, this requirement might not create an unreasonable burden. In the State of California, however, with more than 45,000 peace officers authorized to have access to criminal history information, and with thousands of other persons involved in the criminal justice system also authorized to have access, it would be an impossible task merely to update the list of persons authorized to have access. If implemented such a provision would virtually destroy the ability of the California Department of Justice to handle the exchange of criminal justice information in the state. This would be true despite the fact that California has stringent safeguards to protect individual privacy and the security of the records which are disseminated.

Our more detailed discussion of S. 3418 is contained in the attached "Critique of S. 3418." I wish to thank you for taking the time to solicit our views on this matter, and wish to offer the assistance of our staff, which has considerable expertise in this area, should you desire it.

Very truly yours,

EVEILLE J. YOUNGER,
Attorney General.

Enc. Critique of S. 3418
California Criminal Records Law
Assembly Bill 2656

CRITIQUE OF S. 3418

Our review of S. 3418 gives rise to the following comments:

Section 103(3) appears to authorize the federal Privacy Board to delegate its authority to a state agency. However, there are no criteria set up for determining the type of agency to which this authority would be delegated. We believe that this authority should only be delegated to agencies with expertise in this area. For example, local law enforcement agencies should be responsible to a state Department of Justice or similar agency rather than to a non-criminal justice agency which does not follow the same security and use standards as do criminal justice agencies.

Section 201(a)(3) speaks of establishing "categories" for maintaining personal information to operate in conjunction with confidentiality requirements and access controls. We are uncertain as to what is meant by establishing "categories" and believe that this concept should be better defined.

Section 201(a)(6) prohibits the transfer of personal information beyond the jurisdiction of the United States without specific authority from the subject or pursuant to a treaty or executive agreement. This section might cause little problem for states which do not have borders contiguous with foreign jurisdictions. However, California borders on Mexico and has substantial criminal justice contacts with Mexico. To our knowledge there are no treaties authorizing transfer of this type of information, and this proposal would prohibit us from working with the Mexican authorities in protecting the general public from criminal activity which routinely operates on both sides of the border. This is especially true in regard to drug traffic.

Sections 201(a)(8) and (9) require that lists be maintained of all persons having access to criminal information systems. As was discussed in the Attorney General's letter, this would require the Department of Justice in California, the largest state in the union, to maintain lists containing tens of thousands of names. It would impose an impossible administrative burden upon the department. This provision is unnecessary in California because access and dissemination of criminal records are strictly controlled by state law and policy.

Section 201(a)(13) prohibits the collection of personal information concerning the political and religious beliefs or affiliations and activities of data subjects unless authorized by law. Although we agree that information of this nature should not be maintained absent a compelling reason, we are all aware that there are quasi-political and religious groups which engage in violent criminal activity. Although in California some agencies are authorized by law to maintain information on such groups, this restriction could raise serious doubts as to the ability of many law enforcement agencies to maintain information on such groups as the Symbionese Liberation Army, and the Weathermen Underground. In addition, it appears to prohibit law enforcement personnel from obtaining the religious background or political affiliation of a person who comes into contact with the criminal justice system, even though this information may be of assistance in apprehending a fugitive from justice. An exception for legitimate law enforcement use of this information should be written into the law.

Section 201(b)(1)(B) prohibits the dissemination for independent analysis of statistical materials without guarantees that personal information will not be used in a way that might prejudice judgments about a data subject. Quite often in California statistical information pertaining to individuals is released to chiefs of police, district attorneys, probation officers, and judges to assist them in better performing their functions. For example, information concerning persons placed on probation in Los Angeles County for a certain period of time might be released. This allows local agencies to determine the success of programs, and to isolate those individuals who have proven to be unresponsive to rehabilitative treatment. The public interest requires that this type of information be disseminated, and this provision should be amended to authorize such activity.

Section 201(b)(2)(C) appears to prohibit any federal agency from transmitting a private statistical study or other compilation of information derived by mechanical or electronic means from any file containing personal information. This section may interfere with the ability of such agencies as the FBI to transmit confidential crime report information to the states or to local jurisdictions. This obviously would not be in the public interest and serious consideration should be given to amending the section to authorize that type of transmission.

Section 201(c) requires public notice of the existence of information systems. Although it may cause problems for highly confidential law enforcement information systems because of publicity surrounding the notice of their existence, we believe that it is in the interest of sound government that people know such systems exist.

Sections 201(c)(5)(H), (I); Sections 201(d)(1), (3), (4) would authorize an individual to have complete access to any file maintained on him by a criminal justice agency. Some types of files, such as criminal history files, should be accessible to the subject, and accessible under California law. However, the public interest requires that investigatory material be kept confidential. For example, in attempting to combat organized crime, the Organized Crime and Criminal Intelligence Bureau of the California Department of Justice maintains confidential files on known organized crime figures. It is essential that this information be kept confidential because its disclosure would assist subjects to take courses of action which would avoid detection by the law, and because informants and other sources of information would be disclosed to the subjects. We feel that there is no doubt in any reasonable mind but that in some situations information should be kept confidential and urge that this statute exempt law enforcement files, or at least those which must be kept confidential, from its provisions. As is noted below the existing exemption section is inadequate. If there is concern over the content of confidential records, other types of controls such as official audit and purge procedures should be instituted.

Section 201(d)(1) requires that an individual asked to supply information be given certain explanatory information concerning whether or not he is required to supply the information by law and the consequences of providing or not providing information. This section exemplifies the need for making a distinction between criminal justice records and non-criminal justice records. Although this requirement may make sense when dealing with non-criminal justice information systems where initial contact is voluntary, it makes little sense to inform a person who has been arrested for a crime that he is required to give certain identifying information, and it is virtually impossible to tell him what the possible legal and factual consequences of supplying the information are.

Sections 201(d)(5)(A), (B), (C), (D), (E), (F), (G) authorize an individual to challenge a record and to include an explanatory statement in a record. For the reasons discussed above, this procedure should not be applied to confidential records. If the subject is allowed to review the records in order to challenge them, he or she will in effect have breached the confidentiality of the records.

In terms of criminal history records, California has a better system for resolving disputes, and it is suggested that federal legislation in this area should allow for local variations. For example, in California rather than filing an unverified 200-word statement, the subject may have the entire record adjudicated through an administrative procedure which will factually settle the dispute over the accuracy of the record.

Section 201(e) requires that within two years of the passage of S. 3418 every record system must inform every subject on whom information is maintained of the fact that the record exists. It also requires that the notice explain the type of information contained in the record, and inform the subject of the place where the record is being maintained.

In some cases this provision is inconsistent with the public interest in that it would breach the confidentiality and security of certain records. In other cases, where the record need not be kept confidential, it would impose an impossible burden upon the public agency. In California it would probably require contacting millions of persons at substantial expense to the state. The advantage to be gained from such an expenditure is questionable. When dealing in the area of criminal records it is reasonable to assume that persons who come into contact with the criminal justice system know that records are being maintained upon them. In California, for example, if a person wishes to know whether or not a criminal history is being maintained he or she may write to the California Department of Justice. To mandate that California or any other state send out millions of notices to persons on whom criminal records may be maintained is to mandate a substantial waste of taxpayer's money which will accomplish very little in terms of furthering individual rights of privacy. We make no comment as to whether or not this would be of value in a privately maintained information system.

Section 202. As we have indicated both in the covering letter and in this statement, we believe that the provisions of this section should not apply to confidential criminal records. There is a strong public interest in ensuring that certain types of criminal activity are prohibited, and we should not compromise confidential information systems by laws which may or may not be of value to the individual. We strongly urge that this section be expanded to exclude all investigatory files. The present exception is too restrictive. It applies the provisions of the bill to investigatory files which are "maintained for a period longer than is necessary to commence criminal prosecution." In dealing with organized criminal activity, criminal intelligence information may be maintained for years before there is sufficient information to prosecute the subject. In other cases a completed investigatory file may contain information concerning informants or other persons or situations which must be kept confidential for the safety of the informant, the security of further investigations, or in order to protect the reputation of innocent persons. Applying the standard in section 202 to such needed and important files would require that they be disclosed to the subject thus destroying the ability of the law enforcement agency involved to adequately protect the public from criminal activity, as well as endangering the life or reputation of other persons.

CALIFORNIA CRIMINAL RECORDS LAW

Existing California law does the following:

1. Expressly states who is entitled to receive criminal history information (Penal Code Section 11105).

2. Requires detailed disposition reporting (Penal Code Sections 11115 - 11117; 13100 - 13202).

3. Authorizes subject of criminal history record to review record and to correct errors (Penal Code Sections 11120 - 11127).

4. Requires California Department of Justice to establish statewide standards for criminal history record security and privacy (Penal Code Sections 11075 - 11081).

5. Authorizes sealing of records pertaining to arrests or convictions of minors for misdemeanors or to juvenile court matters (Penal Code Sections 1203.45; Penal Code Section 851.7; Welfare and Institutions Code Section 781).

6. Makes it a crime to maliciously communicate the fact that a person is on parole or is a discharged prisoner with intent to deprive him of employment (Penal Code Sections 2947; 3058).

Proposed California Law:

To make unauthorized dissemination of criminal history information a crime (Assembly Bill 1687; passage expected, to be effective January 1, 1975).

California Department of Justice Policy:

The California Department of Justice has implemented a record retention schedule which will purge from state central files information which is of little use to the criminal justice system. After appropriate experience at the state level, it is anticipated that this criteria will be applied to all criminal justice agencies in the state (see Record Retention Criteria, enclosed).

EXISTING CALIFORNIA LAW

Article 3

CRIMINAL IDENTIFICATION AND STATISTICS

Sec.

11100. Modus operandi cards.
11101. Photographs, descriptions, measurements, etc.
11102. Identification systems.
11103. Duplicate record of all convicts.
11104. Duty to file and index information received.
11105. Information furnished; application; purpose.
11105.5 Notice to officers and agents that record of minor has been sealed.
11106. Records of fingerprints, weapons transactions, pawned property, etc.; copies of records.
11107. Reports of sex crimes and of all felonies.
11108. Reports of lost, stolen, found, pledged, or pawned property.
11109. Repealed.
11110. Record of reports of suspected infliction of physical injury upon minor and arrests for and convictions of violation of section 273a.
11111. Repealed.
11112. Fingerprints and descriptions of persons arrested for certain offenses; daily reports.
11113. Fingerprints and description of decedents furnished by coroner.
11114. Repealed.

§ 11100. Modus operandi cards

The Attorney General shall provide for the installation of a proper system and file in the office of the bureau, cards containing an outline of the method of operation employed by criminals in the commission of crime.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

§ 11101. Photographs, descriptions, measurements, etc.

The Attorney General shall procure from any available source, and file for record and report in the office of the bureau, all plates, photos, outline pictures, descriptions, information and measurements of all persons convicted of a felony, or imprisoned for violating any of the military, naval, or criminal laws of the United States of America, and of all well-known and habitual criminals.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

§ 11102. Identification systems

The bureau may use the following systems of identification: the Bertillon, the fingerprint system and any system of measurement that may be adopted by law in the various penal institutions of the State.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

§ 11103. Duplicate record of all convicts

The Attorney General shall keep on file in the office of the bureau a record consisting of duplicates of all measurements, processes, operations, signaletic cards, plates, photographs, outline pictures, measurements and descriptions of all persons confined in penal institutions of the State as far as possible, in accordance with whatever system or systems may be commonly used in the State.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

Cross References

Fingerprints, photographs, and additional information from director of corrections, see § 2082.
Notice of release of person convicted of arson, see § 11150.
Registration of sex offenders, see § 290.
Report of pardon, see § 4852.17.

§ 11104. Duty to file and index information received

The Attorney General shall file all plates, photographs, outline pictures, measurements, information and descriptions received and shall make a complete and systematic record and index, providing a method of convenience, consultation and comparison.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

§ 11105. Information furnished; application; purpose

(a) The Attorney General shall furnish, upon application in accordance with the provisions of subdivision (b) of this section, copies of all information pertaining to the identification of any person, such as a plate, photograph, outline picture, description, measurement, or any data about such person of which there is a record in the office of the bureau.

(b) Such information shall be furnished to all peace officers, district attorneys, probation officers, and courts of the state, to United States officers or officers of other states, territories, or possessions of the United States, or peace officers of other countries duly authorized by the Attorney General to receive the same, and to any public defender or attorney representing such person in proceedings upon a petition for certificate of rehabilitation and pardon pursuant to Section 4852.08, upon application in writing accompanied by a certificate signed by the peace officer, public defender, or attorney, stating that the information applied for is necessary for the due administration

of the laws, and not for the purpose of assisting a private citizen in carrying on his personal interests or in maliciously or uselessly harassing, degrading or humiliating any person.

(c) Such information shall not be furnished to any persons other than those listed in subdivision (b) of this section or as provided by law; provided, that such information may be furnished to any state agency, officer, or official when needed for the performance of such agency's, officer's, or official's functions.

(d) Whenever a request for information pertains to a person whose fingerprints are on file with the department and whose record contains no reference to criminal activity, and the information requested is to be used for employment, licensing, or certification purposes, the fingerprint card accompanying such request for information, if any, may be stamped "No criminal record" and returned to the submitting agency.

(e) Whenever information furnished pursuant to this section is to be used for employment, licensing, or certification purposes, the Department of Justice shall charge the requesting agency a fee which it determines to be sufficient to reimburse the department for the cost of furnishing the information, provided that no fee shall be charged a public law enforcement agency for records furnished to assist it in employing, licensing, or certifying a person who is applying for employment with the agency as a peace officer or criminal investigator. Any state agency required to pay a fee to the Department of Justice for information received under this section may charge its applicants a fee sufficient to reimburse the agency for such expense. All moneys received by the department pursuant to this section, Section 12054 of the Penal Code, and Section 13588 of the Education Code are hereby appropriated, without regard to fiscal years, for the support of the Department of Justice in addition to such other funds as may be appropriated therefor by the Legislature.

(f) Whenever there is a conflict, the processing of criminal fingerprints shall take priority over the processing of applicant's fingerprints.

(Added by Stats.1953, c. 1385, p. 2966, § 1. Amended by Stats.1957, c. 2263, p. 3966, § 1; Stats.1967, c. 1519, p. 3614, § 1; Stats.1971, c. 1309, p. —, § 2, urgency, eff. Nov. 1, 1971.)

Cross References

Mental health information to bureau of criminal identification and investigation, see Welfare and Institutions Code § 5328.2.

§ 11105.5 Notice to officers and agents that record of minor has been sealed

When the Bureau of Criminal Identification and Investigation receives a report that the record of a minor has been sealed under Section 851.7 or Section 1203.45 of the Penal Code, it shall send notice

of that fact to all officers and agencies that it had previously notified of the arrest or other proceedings against the minor.

(Added by Stats.1965, c. 1910, p. 4422, § 2. Amended by Stats.1967, c. 1373, p. 3224, § 3.)

§ 11106. Records of fingerprints, weapons transactions, pawned property, etc.; copies of records

In order to assist in the investigation of crime, the arrest and prosecution of criminals and the recovery of lost, stolen, or found property, the Attorney General shall keep and properly file a complete record of all copies of fingerprints, duplicate carbon copies of applications for licenses to carry concealed weapons and dealers' records of sales of deadly weapons, and reports of stolen, lost, found, pledged, or pawned property in any city or county of this State and shall furnish copies of any of such records to the officers mentioned in Section 11105 upon proper application therefor.

(Added by Stats.1953, c. 1385, p. 2966, § 1.)

Cross References

Fingerprints, photographs, and additional information from director of corrections, see § 2082.

Fingerprints of applicants for licenses to carry concealed weapons, see § 12052.

Register of sale of concealed weapon to be forwarded to state bureau of criminal identification and investigation, see § 12076.

§ 11107. Reports of sex crimes and of all felonies

Each sheriff, chief of police and city marshal shall furnish to the bureau daily reports on standard forms to be prepared by the bureau listing all violations of Sections 314, 647a, subdivision (a) or (d) of Section 647, and any offense involving lewd and lascivious conduct under Section 272, and all felonies committed in his jurisdiction, describing the nature and character and noting all peculiar circumstances of each such crime together with any additional or supplemental data or information including all statements and conversations of persons arrested, and listing any crime theretofore reported which may be of aid in the investigation of such crime and the apprehension and conviction of the perpetrators thereof.

(Added by Stats.1953, c. 1385, p. 2965, § 1. Amended by Stats.1969, c. 43, p. 155, § 4.)

§ 11108. Reports of lost, stolen, found, pledged, or pawned property

Each sheriff, chief of police or city marshal shall furnish the bureau daily reports of lost, stolen, found, pledged or pawned property received in his office, and all information received from the reports submitted pursuant to Section 21208 of the Financial Code.

(Added by Stats.1953, c. 1385, p. 2967, § 1. Amended by Stats.1959, c. 638, p. 2616, § 6.)

§ 11109. Repealed by Stats.1955, c. 1128, p. 2121, § 1

§ 11110. Record of reports of suspected infliction of physical injury upon minor and arrests for and convictions of violation of section 273a

The State Bureau of Criminal Identification and Investigation shall maintain records of all reports of suspected infliction of physical injury upon a minor by other than accidental means and reports of arrests for, and convictions of, violation of Section 273a. On receipt from a city police department, sheriff or district attorney of a copy of a report of suspected infliction of physical injury upon a minor by other than accidental means received from a physician and surgeon, dentist, resident, intern, chiropractor, religious practitioner, registered nurse employed by a public health agency, school, or school district, director of a county welfare department, or any superintendent of schools of any public or private school system or any principal of any public or private school, the bureau shall transmit to the city police department, sheriff or district attorney, information detailing all previous reports of suspected infliction of physical injury upon the same minor or another minor in the same family by other than accidental means and reports of arrests for, and convictions of violation of Section 273a, concerning the same minor or another minor in the same family.

The bureau may adopt rules governing recordkeeping and reporting under Section 11161.5.

(Added by Stats.1965, c. 1171, p. 2971, § 1. Amended by Stats.1966, 1st Ex.Sess., c. 31, p. 325, § 1; Stats.1968, c. 587, p. 1258, § 1.)

§ 11111. Repealed by Stats.1955, c. 1128, p. 2121, § 1

§ 11112. Fingerprints and descriptions of persons arrested for certain offenses; daily reports

The first agency to receive a person for booking after his arrest shall furnish the bureau daily copies of fingerprints on standardized eight- by eight-inch cards, and descriptions of: (a) all persons who have been arrested for the commission of any offense defined in Section 266, 267, 268, 285, 286, 288, 288a, 314, 647a, subdivision (a) or (d) of Section 647, subdivision 3 or 4 of Section 261, or of any offense involving lewd and lascivious conduct under Section 272; (b) all persons arrested who in the best judgment of any such officer are wanted for serious crimes, or are fugitives from justice; (c) all persons in whose possession at the time of arrest are found goods or property reasonably believed by any such officers to have been stolen by them; (d) all persons in whose possession are found burglar outfits or burglar keys or who have in their possession high-power explosives reasonably believed to be used or intended to be used for unlawful

purposes; (e) all persons who are in possession of infernal machines, bombs or other contrivances in whole or in part and reasonably believed by any said officer to be used or intended to be used for unlawful purposes; (f) all persons who carry concealed firearms or other deadly weapons which are reasonably believed to be carried for unlawful purposes; (g) all persons who have in their possession inks, dye, paper or other articles necessary in the making of counterfeit banknotes, or in the alteration of banknotes, checks, drafts or other instruments of credit; or dies, molds or other articles necessary in the making of counterfeit money, and reasonably believed to be used or intended to be used by them for such unlawful purposes.

(Added by Stats.1953, c. 1385, p. 2967, § 1. Amended by Stats.1968, c. 377, p. 789, § 1; Stats.1969, c. 43, p. 155, § 5.)

Cross References

Fingerprints from director of corrections, see § 2082.

§ 11113. Fingerprints and description of decedents furnished by coroner

Each coroner shall furnish the bureau promptly with copies of fingerprints on standardized 8-inch by 8-inch cards, and descriptions and other identifying data, including date and place of death, of all deceased persons whose deaths are in classifications requiring inquiry by the coroner. When it is not physically possible to furnish prints of the 10 fingers, prints or partial prints of any fingers, with other identifying data, shall be forwarded by the coroner to the bureau.

In all cases where there is a criminal record on file in the bureau for the decedent, the bureau shall notify the Federal Bureau of Investigation and each California sheriff and chief of police, in whose jurisdiction the decedent has been arrested, of the date and place of death of decedent.

(Added by Stats.1963, c. 1665, p. 3256, § 1.)

§ 11114. Repealed by Stats.1955, c. 1128, p. 2121, § 1

Article 4

CRIMINAL RECORDS

Sec.

11115. Report on transfer, release, or disposition of case to bureau of criminal identification and investigation or F.B.I.
11116. Report on disposition of case; disposition labels.
11116.5 Use of disposition label by defendant.
11116.6 Entry of disposition labels on records.
11117. Procedures and forms; record of disposition; time for forwarding reports; inadmissible in civil cases.

§ 11115. Report on transfer, release, or disposition of case to bureau of criminal identification and investigation or F.B.I.

In any case in which a sheriff, police department or other law enforcement agency makes an arrest and transmits a report of the arrest to the Bureau of Criminal Identification and Investigation or to the Federal Bureau of Investigation, it shall be the duty of such law enforcement agency to furnish a disposition report to such bureaus whenever the arrested person is transferred to the custody of another agency or is released without having a complaint or accusation filed with a court.

If either of the following dispositions is made, the disposition report shall so state:

(a) "Arrested for intoxication and released," when the arrested party is released pursuant to paragraph (2) of subdivision (b) of Section 849.

(b) "Detention only," when the detained party is released pursuant to paragraph (1) of subdivision (b) of Section 849. In such cases the report shall state the specific reason for such release, indicating that there was no ground for making a criminal complaint because (1) further investigation exonerated the arrested party, (2) the complainant withdrew the complaint, (3) further investigation appeared necessary before prosecution could be initiated, (4) the ascertainable evidence was insufficient to proceed further, (5) the admissible or adducible evidence was insufficient to proceed further, or (6) other appropriate explanation for release.

When a complaint or accusation has been filed with a court against such an arrested person, the law enforcement agency having primary jurisdiction to investigate the offense alleged therein shall receive a disposition report of that case from the appropriate court and shall transmit a copy of the disposition report to all the bureaus to which arrest data has been furnished.

(Added by Stats.1961, c. 1025, p. 2709, § 1. Amended by Stats.1967, c. 1519, p. 3614, § 2.)

§ 11116. Report on disposition of case; disposition labels

Whenever a criminal complaint or accusation is filed in any superior, municipal or justice court, the clerk, or, if there be no clerk, the judge of that court shall furnish a disposition report of such case to the sheriff, police department or other law enforcement agency primarily responsible for the investigation of the crime alleged in a form prescribed or approved by the Bureau of Criminal Identification and Investigation.

The disposition report shall state one or more of the following, as appropriate:

(a) "Dismissal in furtherance of justice, pursuant to Section 1385 of the Penal Code." In addition to this disposition label, the court

shall set forth the particular reasons for the dismissal as stated in its order entered upon the minutes.

(b) "Case compromised; defendant discharged because restitution or other satisfaction was made to the injured person, pursuant to Sections 1377 and 1378 of the Penal Code."

(c) "Court found insufficient cause to believe defendant guilty of a public offense; defendant discharged without trial pursuant to Section 871 of the Penal Code."

(d) "Dismissal due to delay; action against defendant dismissed because the information was not filed or the action was not brought to trial within the time allowed by Section 1381, 1381.5, or 1382 of the Penal Code.

(e) "Accusation set aside pursuant to Section 995 of the Penal Code." In addition to this disposition label, the court shall set forth the particular reasons for the disposition.

(f) "Defective accusation; defendant discharged pursuant to Section 1008 of the Penal Code," when the action is dismissed pursuant to that section after demurrer is sustained, because no amendment of the accusatory pleading is permitted or amendment is not made or filed within the time allowed.

(g) "Defendant became a witness for the people and was discharged pursuant to Section 1099 of the Penal Code."

(h) "Defendant discharged at trial because of insufficient evidence, in order to become a witness for his codefendant pursuant to Section 1100 of the Penal Code."

(i) "Proceedings suspended; defendant found presently insane and committed to state hospital pursuant to Sections 1367 to 1372 of the Penal Code." If defendant later becomes sane and is legally discharged pursuant to Section 1372, his disposition report shall so state.

(j) "Convicted of (state offense)." The disposition report shall state whether defendant was convicted on plea of guilty, on plea of nolo contendere, by jury verdict, or by court finding and shall specify the sentence imposed, including probation granted, suspension of sentence, imposition of sentence withheld, or fine imposed, and if fine was paid.

(k) "Acquitted of (state offense)," when a general "not guilty" verdict or finding is rendered.

(l) "Not guilty by reason of insanity," when verdict or finding is that defendant was insane at the time the offense was committed.

(m) "Acquitted; proof at trial did not match accusation," when defendant is acquitted by reason of variance between charge and proof pursuant to Section 1151.

(n) "Acquitted; previously in jeopardy," when defendant is acquitted on a plea of former conviction or acquittal or once in jeopardy pursuant to Section 1151.

(o) "Judgment arrested; defendant discharged," when the court finds defects in the accusatory pleading pursuant to Sections 1185 to 1187, and defendant is released pursuant to Section 1188.

(p) "Judgment arrested; defendant recommitted," when the court finds defects in the accusatory pleading pursuant to Sections 1185 to 1187, and defendant is recommitted to answer a new indictment or information pursuant to Section 1188.

(q) "Mistrial; defendant discharged." In addition to this disposition label, the court shall set forth the particular reasons for its declaration of a mistrial.

(r) "Mistrial; defendant recommitted." In addition to this disposition label, the court shall set forth the particular reasons for its declaration of a mistrial.

(s) Any other disposition by which the case was terminated. In addition to the disposition label, the court shall set forth the particular reasons for the disposition.

Whenever a court shall dismiss the accusation or information against a defendant under the provisions of Section 1203.4 of this code, and whenever a court shall order the record of a minor sealed under the provisions of Section 851.7 or Section 1203.45 of this code, the clerk, or, if there be no clerk, the judge of that court shall furnish a report of such proceedings to the Bureau of Criminal Identification and Investigation and shall include therein such information as may be required by said bureau.

(Added by Stats.1961, c. 1025, p. 2709, § 1. Amended by Stats.1965, c. 1910, p. 4422, § 3; Stats.1967, c. 1373, p. 3225, § 4; Stats.1967, c. 1519, p. 3617, § 3.5.)

§ 11116.5 Use of disposition label by defendant

Any disposition label provided by Section 11115 or 11116 may be used by the person subject to the disposition as an answer to any question regarding his arrest or detention history or any question regarding the outcome of a criminal proceeding against him.

(Added by Stats.1967, c. 1519, p. 3619, § 4.)

§ 11116.6 Entry of disposition labels on records

The disposition labels provided by Sections 11115 and 11116 must be entered on all appropriate records of the party arrested, detained, or against whom criminal proceedings are brought.

(Added by Stats.1967, c. 1519, p. 3619, § 5.)

§ 11117. Procedures and forms; record of disposition; time for forwarding reports; inadmissible in civil cases

The Bureau of Criminal Identification and Investigation shall prescribe and furnish the procedures and forms to be used for the disposi-

tion reports required in this article. The bureau shall add the disposition reports received to all appropriate criminal records.

The disposition reports required in this article shall be forwarded to the Bureau of Criminal Identification and Investigation and the Federal Bureau of Investigation within 30 days after the release of the arrested or detained person or the termination of court proceedings.

Neither the disposition reports nor the disposition labels required in this article shall be admissible in evidence in any civil action.

(Added by Stats.1961, c. 1025, p. 2710, § 1. Amended by Stats.1967, c. 1519, p. 3619, § 6.)

Article 5

EXAMINATION OF RECORDS

Sec.

11120. Record defined.
11121. Purpose.
11122. Application; contents; fee.
11123. Submission of application; fee.
11124. Notice of existence of record; time of inspection; examination; authority to take notes.
11125. Application of prisoner; place of examination of record.
11126. Correction of record; written request for clarification; notice to applicant of determination; administrative adjudication; judicial review.
11127. Regulations.

§ 11120. Record defined

As used in this article, "record" with respect to any person means the master record sheet maintained under such person's name by the Bureau of Criminal Identification and Investigation, and which is commonly known as "arrest record," "criminal record sheet," or "rap sheet." "Record" does not include any other records of the bureau.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11121. Purpose

It is the function and intent of this article to afford persons concerning whom a record is maintained in the files of the bureau such reasonable opportunity to examine the record compiled from such files, and to refute any erroneous or inaccurate information contained therein as is consistent with the requirements and functions of the bureau.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11122. Application; contents; fee

Any person desiring to examine a record relating to himself shall obtain from the chief of police of the city of his residence, or, if not

a resident of a city, from the sheriff of his county of residence, or from the office of the bureau, an application form furnished by the bureau which shall require his fingerprints in addition to such other information as the bureau shall specify. The city or county, as applicable, may fix a reasonable fee for affixing the applicant's fingerprints to the form, and shall retain such fee for deposit in its treasury.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11123. Submission of application; fee

The applicant shall submit the completed application directly to the bureau. The application shall be accompanied by a fee of five dollars ($5) or such higher amount, not to exceed ten dollars ($10) that the bureau determines equals the costs of processing the application and making a record available for examination. All fees received by the bureau under this section are hereby appropriated without regard to fiscal years for the support of the Department of Justice in addition to such other funds as may be appropriated therefor by the Legislature.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11124. Notice of existence of record; time of inspection; examination; authority to take notes

When an application is received by the bureau, the bureau shall determine whether a record pertaining to the applicant is maintained. If such record is maintained, the bureau shall inform the applicant by mail of the existence of the record and shall specify a time when the record may be examined at a suitable facility of the bureau. Upon verification of his identity, the applicant shall be allowed to examine the record pertaining to him, or a true copy thereof, for a period not to exceed one hour. The applicant may not retain or reproduce the record, but he may make a written summary or notes in his own handwriting.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11125. Application of prisoner; place of examination of record

If the applicant is imprisoned in the state prison or confined in the county jail, his application shall be through the office in charge of records of the prison or jail. Such offices shall follow the provisions of this article applicable to cities and counties with respect to applications and fees. When an application is transmitted to the bureau pursuant to this section, the bureau shall make arrangements for the applicant to examine the record at his place of confinement. In all other respects, the provisions of Section 11124 shall govern the examination of the record.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11126. Correction of record; written request for clarification; notice to applicant of determination; administrative adjudication; judicial review

(a) If the applicant desires to question the accuracy or completeness of any matter contained in the record, he may submit a written request, to the bureau in a form established by it. The request shall include a statement of the alleged inaccuracy or incompleteness in the record, and specify any proof or corroboration available. Upon receipt of such request, the bureau shall forward it to the person or agency which furnished the questioned information. Such person or agency shall, within 30 days of receipt of such written request for clarification, review its information and forward to the bureau the results of such review.

(b) If such agency concurs in the allegations of inaccurateness or incompleteness in the record, it shall correct its record and shall so inform the bureau, which shall correct the record accordingly. The bureau shall inform the applicant of its correction of the record under this subdivision within 30 days.

(c) If such agency denies the allegations of inaccurateness or incompleteness in the record, the matter shall be referred for administrative adjudication in accordance with Chapter 5 (commencing with Section 11500) of Part 1, Division 3, Title 2 of the Government Code for a determination of whether inaccuracy or incompleteness exists in the record. The agency from which the questioned information originated shall be the respondent in the hearing. If an inaccuracy or incompleteness is found in any record, the agency in charge of that record shall be directed to correct it accordingly. Judicial review of the decision shall be governed by Section 11523 of the Government Code. The applicant shall be informed of the decision within 30 days of its issuance in accordance with Section 11518 of the Government Code.

(Added by Stats.1971, c. 1439, p. —, § 1.)

§ 11127. Regulations

The bureau shall adopt all regulations necessary to carry out the provisions of this article.

(Added by Stats.1971, c. 1439, p. —, § 1.)

ARTICLE 2.5. CRIMINAL RECORD DISSEMINATION [NEW]

Sec.

11075. Criminal offender record information.
11076. Dissemination to authorized agencies.
11077. Attorney general; duties.
11078. Listing of agencies to whom information released or communicated.
11079. Investigations; cooperation by agencies.
11080. Right of access to information authorized by other provisions of law not affected.
11081. No access to information unless otherwise authorized by law.

Article 2.5 was added by Stats.1972, c. 1437, p. —, § 1.

§ 11075. Criminal offender record information

(a) As used in this article, "criminal offender record information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.

(b) Such information shall be restricted to that which is recorded as the result of an arrest, detention, or other initiation of criminal proceedings or of any consequent proceedings related thereto.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11076. Dissemination to authorized agencies

Criminal offender record information shall be disseminated, whether directly or through any intermediary, only to such agencies as are, or may subsequently be, authorized access to such records by statute.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11077. Attorney general; duties

The Attorney General is responsible for the security of criminal offender record information. To this end, he shall:

(a) Establish regulations to assure the security of criminal offender record information from unauthorized disclosures at all levels of operation in this state.

(b) Establish regulations to assure that such information shall be disseminated only in situations in which it is demonstrably required for the performance of an agency's or official's functions.

(c) Coordinate such activities with those of any interstate systems for the exchange of criminal offender record information.

37-583 O - 74 - pt. 2 - 34

(d) Cause to be initiated for employees of all agencies that maintain, receive, or are eligible to maintain or receive, criminal offender record information a continuing educational program in the proper use and control of criminal offender record information.

(e) Establish such regulations as he finds appropriate to carry out his functions under this article.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11078. Listing of agencies to whom information released or communicated

Each agency holding or receiving criminal offender record information in a computerized system shall maintain, for such period as is found by the Attorney General to be appropriate, a listing of the agencies to which it has released or communicated such information.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11079. Investigations; cooperation by agencies

The Attorney General may conduct such inquiries and investigations as he finds appropriate to carry out functions under this article. He may for this purpose direct any agency that maintains, or has received, or that is eligible to maintain or receive criminal offender records to produce for inspection statistical data, reports, and other information concerning the storage and dissemination of criminal offender record information. Each such agency is authorized and directed to provide such data, reports, and other information.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11080. Right of access to information authorized by other provisions of law not affected

Nothing in this article shall be construed to affect the right of access of any person or public agency to individual criminal offender record information that is authorized by any other provision of law.

(Added by Stats.1972, c. 1437, p. —, § 1.)

§ 11081. No access to information unless otherwise authorized by law

Nothing in this article shall be construed to authorize access of any person or public agency to individual criminal offender record information unless such access is otherwise authorized by law.

(Added by Stats.1972, c. 1437, p. —, § 1.)

ARTICLE 3. CRIMINAL IDENTIFICATION AND STATISTICS

Sec.

11111. Bicycles; stolen and lost; records; accessibility to law enforcement agencies; fees [New].

§ 11102. Identification systems

The department may use the following systems of identification: the Bertillon, the fingerprint system, and any system of measurement that may be adopted by law in the various penal institutions of the state.

(Amended by Stats.1972, c. 1377, p. —, § 82.1.)

§ 11105. Information furnished; application; purpose

(a) The Attorney General shall furnish, upon application in accordance with the provisions of subdivision (b) of this section, copies of all summary criminal history information pertaining to the identification of any person, such as a plate, photograph, outline picture, description, measurement, or any data about such person of which there is a record in the office of the department.

(b) Such information shall be furnished to all peace officers, district attorneys, probation officers, and courts of the state, to United States officers or officers of other states, territories, or possessions of the United States, or peace officers of other countries duly authorized by the Attorney General to receive the same, and to any public defender or attorney representing such person in proceedings upon a petition for certificate of rehabilitation and pardon pursuant to Section 4852.08, upon application in writing accompanied by a certificate signed by the peace officer, public defender, or attorney, stating that the information applied for is necessary for the due administration of the laws, and not for the purpose of assisting a private citizen in carrying on his personal interests or in maliciously or uselessly harassing, degrading or humiliating any person.

(c) Such information shall not be furnished to any persons other than those listed in subdivision (b) of this section or as provided by law; provided, that such information may be furnished to any state agency, officer, or official when needed for the performance of such agency's, officer's, or official's functions.

(d) Whenever a request for information pertains to a person whose fingerprints are on file with the department and whose record contains no reference to criminal activity, and the information requested is to be used for employment, licensing, or certification purposes, the fingerprint card accompanying such request for information, if any, may be stamped "No criminal record" and returned to the submitting agency.

(e) Whenever information furnished pursuant to this section is to be used for employment, licensing, or certification purposes, the Department of Justice shal charge the requesting agency a fee which it determines to be sufficient to reimburse the department for the cost of furnishing the information, provided that no fee shall be charged a public law enforcement agency for records furnished to assist it in employing, licensing, or certifying a person who is applying for employment with the agency as a peace officer or criminal investigator. Any state agency required to pay a fee to the Department of Justice for information received under this section may charge its applicants a fee sufficient to reimburse the agency for such expense. All moneys received by the department pursuant to this section, Section 12054 of the Penal Code, and Section 13588 of the Education Code are hereby appropriated, without regard to fiscal years, for the support of the Department of Justice in addition to such other funds as may be appropriated therefor by the Legislature.

(f) Whenever there is a conflict, the processing of criminal fingerprints shall take priority over the processing of applicant's fingerprints.

(Amended by Stats.1972, c. 1377, p. —, § 82.2.)

§ 11107. Reports of sex crimes and of all felonies

Each sheriff, chief of police and city marshal shall furnish to the department daily reports on standard forms to be prepared by the department listing all violations of Sections 314, 647a, subdivision (a) or (d) of Section 647, and any offense involving lewd and lascivious conduct under Section 272, and all felonies committed in his jurisdiction, describing the nature and character and noting all peculiar circumstances of each such crime together with any additional or supplemental data or information including all statements and conversations of persons arrested, and listing any crime theretofore reported which may be of aid in the investigation of such crime and the apprehension and conviction of the perpetrators thereof.

(Amended by Stats.1972, c. 1377, p. —, § 82.3.)

§ 11110. Record on reports of suspected infliction of physical injury upon minor and arrests for and convictions of violation of section 273a

The Department of Justice shall maintain records of all reports of suspected infliction of physical injury upon a minor by other than accidental means and reports of arrest for, and convictions of, violation of Section 273a. On receipt from a city police department, sheriff or district attorney of a copy of a report of suspected infliction of physical injury upon a minor by other than accidental means received from a physician and surgeon, dentist, resident, intern, chiropractor, religious practitioner, registered nurse employed by a public health agency, school, or school district, director of a county welfare department, or any superintendent of schools of any public or private school system or any principal of any public or private school, the department shall transmit to the city police department, sheriff or district attorney, information detailing all previous reports of suspected infliction of physical injury upon the same minor or another minor in the same family by other than accidental means and reports of arrests for, and convictions of violation of Section 273a, concerning the same minor or another minor in the same family.

The department may adopt rules governing recordkeeping and reporting under Section 11161.5.

(Amended by Stats.1972, c. 1377, p. —, § 83.)

§ 11111. Bicycles; stolen and lost; records; accessibility to law enforcement agencies; fees

The Department of Justice shall maintain records relative to stolen and lost bicycles in the Criminal Justice Information System. Such records shall be accessible to authorized law enforcement agencies through the California Law Enforcement Telecommunications System.

The department shall impose annual fees on cities and counties which have adopted bicycle licensing ordinances or resolutions in such amount as are necessary to finance the operation and maintenance of that portion of the Criminal Justice Information System devoted to the records relative to stolen and lost bicycles. The annual fee imposed by the department on a city or a county shall be paid by the city or county from the fees collected

under its adopted bicycle licensing ordinance or resolution, and shall not exceed 20 cents ($0.20) per bicycle licensed under the ordinance or resolution.

(Added by Stats.1972, c. 885, p. —, § 2, urgency, eff. Aug. 15, 1972.)

Sections 3 and 3.5 of Stats.1972, c. 885, p. —, provide:

"Sec. 3. The Department of Justice shall conduct a comparative study to evaluate the following:

"(a) The records of stolen and lost bicycles specified in Section 11111 of the Penal Code.

"(b) The need to establish mandatory statewide registration and licensing with the related activities performed by: (1) the state; (2) local governments; (3) dealers; or (4) others.

"(c) The need for a statewide automated registration file or alternatives thereto.

In carrying out the study, the Department of Justice shall seek the advice and assistance of local authorities, bicycle manufacturers and retailers, and bicyclists' organizations.

A progress study report shall be submitted to the Legislature by February 1, 1974.

"Sec. 3.5. The Department of Justice is directed to make all necessary efforts to obtain federal and private funds for the purposes of carrying out its responsibilities under this act and is authorized, with the approval of the Department of Finance, to receive any grants or gifts for such purposes."

§ 11113. Fingerprints and description of decedents furnished by coroner

Each coroner shall furnish the Department of Justice promptly with copies of fingerprints on standardized eight-inch by eight-inch cards, and descriptions and other identifying data, including date and place of death, of all deceased persons whose deaths are in classifications requiring inquiry by the coroner. When it is not physically possible to furnish prints of the 10 fingers, prints or partial prints of any fingers, with other identifying data, shall be forwarded by the coroner to the department.

In all cases where there is a criminal record on file in the department for the decedent, the department shall notify the Federal Bureau of Investigation and each California sheriff and chief of police, in whose jurisdiction the decedent has been arrested, of the date and place of death of decedent.

(Amended by Stats.1972, c. 1377, p. —, § 83.5.)

ARTICLE 4. CRIMINAL RECORDS

Sec.

11116.7 Certificate of disposition; request by defendant; changes [New].

11116.8 Description of charge or charges in original and amended pleadings; disposition labels [New].

11116.9 Additional copies of disposition; fees [New].

§ 11115. Report on disposition of case

In any case in which a sheriff, police department or other law enforcement agency makes an arrest and transmits a report of the arrest to the Department of Justice or to the Federal Bureau of Investigation, it shall be the duty of such law enforcement agency to furnish a disposition report to such agencies whenever the arrested person is transferred to the custody of another agency or is released without having a complaint or accusation filed with a court.

If either of the following dispositions is made, the disposition report shall so state:

(a) "Arrested for intoxication and released," when the arrested party is released pursuant to paragraph (2) of subdivision (b) of Section 849.

(b) "Detention only," when the detained party is released pursuant to paragraph (1) of subdivision (b) of Section 849. In such cases the report shall state the specific reason for such release, indicating that there was no ground for making a criminal complaint because (1) further investigation exonerated the arrested party, (2) the complainant withdrew the complaint, (3) further investigation appeared necessary before prosecution could be initiated, (4) the ascertainable evidence as insufficient to proceed further, (5) the admissible or adducible evidence was insufficient to proceed further, or (6) other appropriate explanation for release.

When a complaint or accusation has been filed with a court against such an arrested person, the law enforcement agency having primary jurisdiction to investigate the offense alleged therein shall receive a disposition report of that case from the appropriate court and shall transmit a copy of the disposition report to all the bureaus to which arrest data has been furnished.

(Amended by Stats.1972, c. 1377, p. —, § 84.)

§ 11116. Report on disposition of case; disposition labels

Whenever a criminal complaint or accusation is filed in any superior, municipal or justice court, the clerk, or, if there be no clerk, the judge of that court shall furnish a disposition report of such case to the sheriff, police department or other law enforcement agency primarily responsible for the investigation of the crime alleged in a form prescribed or approved by the Department of Justice.

The disposition report shall state one or more of the following, as appropriate:

(a) "Dismissal in furtherance of justice, pursuant to Section 1385 of the Penal Code." In addition to this disposition label, the court shall set forth the particular reasons for the dismissal as stated in its order entered upon the minutes.

(b) "Case compromised; defendant discharged because restitution or other satisfaction was made to the injured person, pursuant to Sections 1377 and 1378 of the Penal Code."

(c) "Court found insufficient cause to believe defendant guilty of a public offense; defendant discharged without trial pursuant to Section 871 of the Penal Code."

(d) "Dismissal due to delay; action against defendant dismissed because the information was not filed or the action was not brought to trial within the time allowed by Section 1381, 1381.5, or 1382 of the Penal Code."

(e) "Accusation set aside pursuant to Section 995 of the Penal Code." In addition to this disposition label, the court shall set forth the particular reasons for the disposition.

(f) "Defective accusation; defendant discharged pursuant to Section 1008 of the Penal Code," when the action is dismissed pursuant to that sec-

tion after demurrer is sustained, because no amendment of the accusatory pleading is permitted or amendment is not made or filed within the time allowed.

(g) "Defendant became a witness for the people and was discharged pursuant to Section 1099 of the Penal Code."

(h) "Defendant discharged at trial because of insufficient evidence, in order to become a witness for his codefendant pursuant to Section 1100 of the Penal Code."

(i) "Proceedings suspended; defendant found presently insane and committed to state hospital pursuant to Sections 1367 to 1372 of the Penal Code." If defendant later becomes sane and is legally discharged pursuant to Section 1372, his disposition report shall so state.

(j) "Convicted of (state offense)." The disposition report shall state whether defendant was convicted on plea of guilty, on plea of nolo contendere, by jury verdict, or by court finding and shall specify the sentence imposed, including probation granted, suspension of sentence, imposition of sentence withheld, or fine imposed, and if fine was paid.

(k) "Acquitted of (state offense)," when a general "not guilty" verdict or finding is rendered.

(l) "Not guilty by reason of insanity," when verdict or finding is that defendant was insane at the time the offense was committed.

(m) "Acquitted; proof at trial did not match accusation," when defendant is acquitted by reason of variance between charge and proof pursuant to Section 1151.

(n) "Acquitted; previously in jeopardy," when defendant is acquitted on a plea of former conviction or acquittal or once in jeopardy pursuant to Section 1151.

(o) "Judgment arrested; defendant discharged," when the court finds defects in the accusatory pleading pursuant to Sections 1185 to 1187, and defendant is released pursuant to Section 1188.

(p) "Judgment arrested; defendant recommitted," when the court finds defects in the accusatory pleading pursuant to Sections 1185 to 1187, and defendant is recommitted to answer a new indictment or information pursuant to Section 1188.

(q) "Mistrial; defendant discharged." In addition to this disposition label, the court shall set forth the particular reasons for its declaration of a mistrial.

(r) "Mistrial; defendant recommitted." In addition to this disposition label, the court shall set forth the particular reasons for its declaration of a mistrial.

(s) Any other disposition by which the case was terminated. In addition to the disposition label, the court shall set forth the particular reasons for the disposition.

Whenever a court shall dismiss the accusation or information against a defendant under the provisions of Section 1203.4 of this code, and whenever a court shall order the record of a minor sealed under the provisions of Section 851.7 or Section 1203.45 of this code, the clerk, or, if there be no clerk, the judge of that court shall furnish a report of such proceedings to

the Department of Justice and shall include therein such information as may be required by said department.

(Amended by Stats.1972, c. 1377, p. —, § 85.)

§ 11116.7 Certificate of disposition; request by defendant; changes

Whenever an accusatory pleading is filed in any court of this state alleging a public offense for which a defendant may be punished by incarceration, for a period in excess of 90 days, the court shall furnish upon request of the defendant named therein a certificate of disposition which describes the disposition of the accusatory pleading in that court when such disposition is one described in Section 11116. The certificate of disposition shall be signed by the judge, shall substantially conform with the requirements of Section 11116.8, and the seal of the court shall be affixed thereto.

In the event that the initial disposition of the accusatory pleading is changed, a new disposition certificate showing the changed disposition shall be issued by the court changing the same upon request of the defendant or his counsel of record.

(Added by Stats.1972, c. 1279, p. —, § 1.)

§ 11116.8 Description of charge or charges in original and amended pleadings; disposition labels

The certificate of disposition provided by Section 11116.7 shall describe the charge or charges set forth in the original and any amended accusatory pleading, together with the disposition of each charge in the original and any amended accusatory pleading by stating one or more of the disposition labels, as appropriate, set forth in Section 11116.

(Added by Stats.1972, c. 1279, p. —, § 2.)

§ 11116.9 Additional copies of disposition; fees

The clerk of the court in which the disposition is made shall provide the defendant or his counsel of record with additional certified copies of the disposition certificate upon the payment of the fees provided by law for certified copies of court records.

(Added by Stats.1972, c. 1279, p. —, § 3.)

§ 11117. Procedures and forms; record of disposition; time for forwarding reports; inadmissible in civil cases

The Department of Justice shall prescribe and furnish the procedures and forms to be used for the disposition reports required in this article. The department shall add the disposition reports received to all appropriate criminal records.

The disposition reports required in this article shall be forwarded to the department and the Federal Bureau of Investigation within 30 days after the release of the arrested or detained person or the termination of court proceedings.

Neither the disposition reports nor the disposition labels required in this article shall be admissible in evidence in any civil action.

(Amended by Stats.1972, c. 1377, p. —, § 86.)

ARTICLE 5. EXAMINATION OF RECORDS

§ 11120. Record defined

As used in this article, "record" with respect to any person means the master record sheet maintained under such person's name by the Department of Justice, and which is commonly known as "arrest record," "criminal record sheet," or "rap sheet." "Record" does not include any other records of the department.

(Amended by Stats.1972, c. 1377, p. —, § 86.1.)

§ 11122. Submission of application; fee

Any person desiring to examine a record relating to himself shall obtain from the chief of police of the city of his residence, or, if not a resident of a city, from the sheriff of his county of residence, or from the office of the department, an application form furnished by the department which shall require his fingerprints in addition to such other information as the department shall specify. The city or county, as applicable, may fix a reasonable fee for affixing the applicant's fingerprints to the form, and shall retain such fee for deposit in its treasury.

(Amended by Stats.1972, c. 1377, p. —, § 86.2.)

§ 11123. Submission of application; fee

The applicant shall submit the completed application directly to the department. The application shall be accompanied by a fee of five dollars ($5) or such higher amount, not to exceed ten dollars ($10) that the department determines equals the costs of processing the application and making a record available for examination. All fees received by the department under this section are hereby appropriated without regard to fiscal years for the support of the Department of Justice in addition to such other funds as may be appropriated therefor by the Legislature.

(Amended by Stats.1972, c. 1377, p. —, § 86.3.)

§ 11124. Notice of existence of record; time of inspection; examination; authority to take notes

When an application is received by the department, the department shall determine whether a record pertaining to the applicant is maintained. If such record is maintained, the department shall inform the applicant by mail of the existence of the record and shall specify a time when the record may be examined at a suitable facility of the department. Upon verification of his identity, the applicant shall be allowed to examine the record pertaining to him, or a true copy thereof, for a period not to exceed one hour. The applicant may not retain or reproduce the record, but he may make a written summary or notes in his own handwriting.

(Amended by Stats.1972, c. 1377, p. —, § 86.4.)

§ 11125. Application of prisoner; place of examination of record

If the applicant is imprisoned in the state prison or confined in the county jail, his application shall be through the office in charge of records of the prison or jail. Such offices shall follow the provisions of this article

applicable to cities and counties with respect to applications and fees. When an application is transmitted to the department pursuant to this section, the department shall make arrangements for the applicant to examine the record at his place of confinement. In all other respects, the provisions of Section 11124 shall govern the examination of the record.

(Amended by Stats.1972, c. 1377, p. —, § 86.5.)

§ 11126. Correction of record; written request for clarification; notice to applicant of determination; administrative adjudication; judicial review

(a) If the applicant desires to question the accuracy or completeness of any matter contained in the record, he may submit a written request, to the department in a form established by it. The request shall include a statement of the alleged inaccuracy or incompleteness in the record, and specify any proof or corroboration available. Upon receipt of such request, the department shall forward it to the person or agency which furnished the questioned information. Such person or agency shall, within 30 days of receipt of such written request for clarification, review its information and forward to the department the results of such review.

(b) If such agency concurs in the allegations of inaccurateness or incompleteness in the record, it shall correct its record and shall so inform the department, which shall correct the record accordingly. The department shall inform the applicant of its correction of the record under this subdivision within 30 days.

(c) If such agency denies the allegations of inaccurateness or incompleteness in the record, the matter shall be referred for administrative adjudication in accordance with Chapter 5 (commencing with Section 11500) of Part 1, Division 3, Title 2 of the Government Code for a determination of whether inaccuracy or incompleteness exists in the record. The agency from which the questioned information originated shall be the respondent in the hearing. If an inaccuracy or incompleteness is found in any record, the agency in charge of that record shall be directed to correct it accordingly. Judicial review of the decision shall be governed by Section 11523 of the Government Code. The applicant shall be informed of the decision within 30 days of its issuance in accordance with Section 11518 of the Government Code.

(Amended by Stats.1972, c. 1377, p. —, § 86.6.)

§ 11127. Regulations

The department shall adopt all regulations necessary to carry out the provisions of this article.

(Amended by Stats.1972, c. 1377, p. —, § 86.7.)

CHAPTER 2. CONTROL OF CRIMES AND CRIMINALS

§ 11150. Release from penal institution, notice

Prior to the release of a person convicted of arson from an institution under the jurisdiction of the Department of Corrections, the Director of Corrections shall notify the State Fire Marshal and the Department of

Operative July 1, 1978.

Provides that neither appropriation is made nor obligation created for the reimbursement of any local agency for any costs incurred by it pursuant to the act.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no state funding.

The people of the State of California do enact as follows:

SECTION 1. Chapter 2 (commencing with Section 13100) is added to Title 3 of Part 4 of the Penal Code, to read:

CHAPTER 2. CRIMINAL OFFENDER RECORD INFORMATION

Article 1. Legislative Findings and Definitions

13100. The Legislature finds and declares as follows:

(a) That the criminal justice agencies in this state require, for the performance of their official duties, accurate and reasonably complete criminal offender record information.

(b) That the Legislature and other governmental policymaking or policy-researching bodies, and criminal justice agency management units require greatly improved aggregate information for the performance of their duties.

(c) That policing agencies and courts require speedy access to information concerning all felony and selected misdemeanor arrests and final dispositions of such cases.

(d) That criminal justice agencies may require regular access to detailed criminal histories relating to any felony arrest that is followed by the filing of a complaint.

(e) That, in order to achieve the above improvements, the recording, reporting, storage, analysis, and dissemination of criminal offender record information in this state must be made more uniform and efficient, and better controlled and coordinated.

13101. As used in this chapter, "criminal justice

agencies" are those agencies at all levels of government which perform as their principal functions, activities which either:

(a) Relate to the apprehension, prosecution, adjudication, incarceration, or correction of criminal offenders; or

(b) Relate to the collection, storage, dissemination or usage of criminal offender record information.

13102. As used in this chapter, "criminal offender record information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.

Such information shall be restricted to that which is recorded as the result of an arrest, detention, or other initiation of criminal proceedings or of any consequent proceedings related thereto. It shall be understood to include, where appropriate, such items for each person arrested as the following:

(a) Personal identification.

(b) The fact, date, and arrest charge; whether the individual was subsequently released and, if so, by what authority and upon what terms.

(c) The fact, date, and results of any pretrial proceedings.

(d) The fact, date, and results of any trial or proceeding, including any sentence or penalty.

(e) The fact, date, and results of any direct or collateral review of that trial or proceeding; the period and place of any confinement, including admission, release; and, where appropriate, readmission and rerelease dates.

(f) The fact, date, and results of any release proceedings.

(g) The fact, date, and authority of any act of pardon or clemency.

(h) The fact and date of any formal termination to the criminal justice process as to that charge or conviction.

(i) The fact, date, and results of any proceeding revoking probation or parole.

It shall not include intelligence, analytical, and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

Article 2. Recording Information

13125. All basic information stored in state or local criminal offender record information systems shall be recorded, when applicable and available, in the form of standard data elements. Such standard data elements shall include, but not be limited to:

The following personal identification data:

- Name—(full name)
  - Aliases
  - Monikers
- Race
- Sex
- Date of birth
- Place of birth (state or country)
- Height
- Weight
- Hair color
- Eye color
- CII number
- FBI number
- Social security number
- California operators license number
- Fingerprint classification number
  - Henry
  - NCIC
- Address

The following arrest data:

- Arresting agency
- Booking number
- Date of arrest
- Offenses charged

Statute citations
Literal descriptions
Police disposition
Released
Turned over to
Complaint filed
The following lower court data:
County and court name
Date complaint filed
Original offenses charged in complaint to superior court.
Held to answer
Certified plea
Disposition—lower court
Not convicted
Dismissed
Acquitted
Court trial
Jury trial
Convicted
Plea
Court trial
Jury trial
Date of disposition
Convicted offenses
Sentence
Proceedings suspended
Reason suspended
The following superior court data:
County
Date complaint filed
Type of proceeding
Indictment
Information
Certification
Original offenses charged in indictment or information
Disposition
Not convicted
Dismissed
Acquitted

Court trial
Jury trial
On transcript
Convicted—felony, misdemeanor
Plea
Court trial
Jury trial
On transcript
Date of disposition
Convicted offenses
Sentence
Proceedings suspended
Reason suspended
Source of reopened cases
The following corrections data:
Adult probation
County
Type of court
Court number
Offense
Date on probation
Date removed
Reason for removal
County jail (sentenced prisoners only)
Name of jail, camp, or other
Convicted offense
Sentence
Date received
Date released
Reason for release
Committing agency
Youth Authority
County
Type of court
Court number
Youth Authority number
Date received
Convicted offense
Type of receipt
Original commitment

Parole violator
Date released
Type of release
Custody
Supervision
Date terminated
Department of Corrections
County
Type of court
Court number
Department of Corrections number
Date received
Convicted offense
Type of receipt
Original commitment
Parole violator
Date released
Type of release
Custody
Supervision
Date terminated
Mentally disordered sex offenders
County
Hospital number
Date received
Date discharged
Recommendation

13126. The Department of Justice shall, when necessary, modify the list of data elements enumerated in Section 13125, in accord with changes in criminal procedures or the organization of criminal justice agencies.

13127. Each recording agency shall insure that each portion of a criminal offender record that it originates shall include, for all felonies and reportable misdemeanors, the state or local unique and permanent fingerprint identification number, within 72 hours of origination of such records, excluding Saturday, Sunday, and holidays.

Article 3. Reporting Information

13150. For each arrest made, the reporting agency shall report to the Department of Justice, concerning each arrest, the applicable identification and arrest data described in Section 13125, including any modification under Section 13126, and fingerprints, except as otherwise provided by law.

13151. The court dispositions of such cases shall be reported by the appropriate agency within 10 days of such disposition. Admissions or releases from detention facilities shall be reported within 10 days of such actions.

13152. Each criminal justice agency filing a complaint subsequent to an arrest where a felony charge is recorded at the time of arrest or booking, and every criminal justice agency taking action towards an offender subsequent to such complaint, shall report, in a form to be determined by the Department of Justice, such information as the Department of Justice requires. The minimum required shall include, but not be limited to, the appropriate data elements enumerated in Section 13125, including any modification under Section 13126, describing those actions initiated or carried out by the agency.

13153. Criminal justice agencies shall report such additional criminal offender record information as the Department of Justice requires, provided that data relating to arrests for being found in any public place under the influence of intoxicating liquor under subdivision (f) of Section 647 shall not be reported or maintained by the Department of Justice without special individual justification.

Article 4. Information Service

13175. When a criminal justice agency supplies fingerprints, or a fingerprint identification number, or such other personal identifiers as the Department of Justice deems appropriate, to the Department of Justice, such agency shall, upon request, be provided with

37-583 O - 74 - pt. 2 - 35

identification, arrest, and, where applicable, final disposition data relating to such person within 72 hours of receipt by the Department of Justice.

13176. When a criminal justice agency entitled to such information supplies fingerprints, or a fingerprint identification number, or such other personal identifiers as the Department of Justice deems appropriate, to the Department of Justice, such agency shall, upon request, be provided with the criminal history of such person, or the needed portion thereof, within 72 hours of receipt by the Department of Justice.

13177. Nothing in this chapter shall be construed so as to prevent the Attorney General from requiring criminal justice agencies to report more information, *if such information is a public record,* than this chapter requires or to record or report it more quickly, or to establish any other regulations *authorized by this chapter or any other provision of law* that would improve ~~the administration of justice.~~ *criminal justice information systems.*

Article 5. Access to Information

13200. Nothing in this chapter shall be construed to affect the right of access of any person or public agency to individual criminal offender record information that is authorized by any other provision of law.

13201. Nothing in this chapter shall be construed to authorize access of any person or public agency to individual criminal offender record information unless such access is otherwise authorized by law.

13202. Every public agency or research body immediately concerned with the prevention or control of crime, the quality of criminal justice, or the custody or correction of offenders shall be provided with such aggregated criminal offender record information as is required for the performance of its duties, or the execution of research projects relating to the activities of criminal justice agencies or changes in legislative or executive policies, insofar as the technical or financial resources of statistical agencies permit, provided that all

material identifying individuals has been removed, and provided that such agency or body pays the cost of the processing of such data when necessary.

SEC. 2. This act shall become operative July 1, 1978.

SEC. 3. No appropriation is made by this act, nor is any obligation created thereby under Section 2164.3 of the Revenue and Taxation Code, for the reimbursement of any local agency for any costs that may be incurred by it in carrying on any program or performing any service required to be carried on or performed by it by this act. This legislation consists of technical changes to statutes enacted prior to January 1, 1973, and therefore does not mandate a local governmental program under Section 2164.3 of the Revenue and Taxation Code.

§ 781. Petition for sealing of records in custody of juvenile court and probation officer, etc.: Effect of order to seal records

In any case in which a petition has been filed with a juvenile court to commence proceedings to adjudge such person a dependent child or ward of the court or in any case in which a person is cited to appear before a probation officer or is taken before a probation officer pursuant to Section 626, or in any case in which a minor is taken before any officer of a law enforcement agency, such person or county probation officer, may, five years or more after the jurisdiction of the juvenile court has terminated as to such person or, in a case in which no petition is filed, five years or more after such person was cited to appear before a probation officer or was taken before a probation officer pursuant to Section 626, or was taken before any officer of a law enforcement agency, or, in any case, at any time after such person has reached the age of 21 years, petition the court for sealing of the records, including records of arrest, relating to such person's case, in the custody of the juvenile court and probation officer and such other agencies, including law enforcement agencies, and public officials, as petitioner alleges, in his petition, to have custody of such records. The court shall notify the district attorney of the county and the county probation officer, if he is not the petitioner of the petition, and such district attorney or probation officer or any of their deputies or any other person having relevant evidence may testify at the hearing on the petition. If, after hearing, the court finds that since such termination of jurisdiction or action pursuant to Section 626, as the case may be, he has not been convicted of a felony or of any misdemeanor involving moral turpitude and that rehabilitation has been attained to the satisfaction of the court, it shall order sealed all records, papers, and exhibits in such person's case in the custody of the juvenile court, including the juvenile court record, minute book entries, and entries on dockets, and other records relating to the case in the custody of such other agencies and officials as are named in the order. Thereafter the proceedings in such case shall be deemed never to have occurred, and such person may properly reply accordingly to any inquiry about the events, records of which are ordered sealed. The court shall send a copy of the order to each agency and official named therein, and each such agency and official shall seal records in its custody as directed by the order, shall advise the court of its compliance, and thereupon shall seal the copy of the court's order for sealing of records that it or he received. The person who is the subject of records sealed pursuant to this section may petition the superior court to permit inspection of the records by persons named in the petition, and the superior court may so order. Otherwise such records shall not be open to inspection.

Note—See Recommendation and Study by California Law Revision Commission, dated October 1960, relating to the right to counsel and the separation of the delinquent from the nondelinquent minor in juvenile court proceedings.

Legislative History:

1. Added by Stats 1961 ch 1616 § 2 p 3493. Based on former § 752, as added by Stats 1959 ch 1723 § 1 p 4132.

2. Amended by Stats 1961 ch 1673 § 2 p 3640, (1) substituting "became" for "has been adjudged" after "in which a person"; (2) adding "for the reasons described in Section 601 or Section 602," after "juvenile court"; (3) substituting "sealing" for "expungement" after "petition the court for"; (4) substituting "sealed" for "expunged" after "it shall order"; (5) adding ", and such former ward may properly reply accordingly to any inquiry about the events, records of which are ordered sealed" after "have occurred"; (6) substituting "seal" for "expunged" after "official shall"; and (7) adding "shall advise the court of its compliance, and thereupon shall seal the copy of the court's order for sealing of records that it or he received. The persons who is the subject of records sealed pursuant to this section may petition the superior court to permit inspection of the records by person named in the petition, and the superior court may so order. Otherwise such records shall not be open to inspection" after "directed by the order."

3. Amended by Stats 1963 ch 1761 § 8 p 3515, substituting "petition has been filed with a juvenile court to commence proceedings to adjudge such person a dependent child or ward of the court" for "person became a ward of the juvenile court for the reasons described in Section 601 or Section 602" after "In any case in which a" at the beginning of the section.

4. Amended by Stats 1965 ch 1413 § 1 p 3330, (1) adding "or in any case in which a person is cited to appear before a probation officer or is taken before a probation officer pursuant to Section 626" after "ward of the court"; (2) adding "or, in a case in which no petition is filed, five years or more after such person was cited to appear before a probation officer or was taken before a probation officer pursuant to Section 626," after "to such person"; (3) adding "or action pursuant to Section 626, as the case may be," after "jurisdiction"; and (4) substituting "person" for "former ward" after "and such."

5. Amended by Stats 1967 ch 1649 § 1 p 3951.

6. Amended by Stats 1967 ch 1650 § 1 p 3952, adding (1) "or in any case in which a minor is taken before any officer of a law enforcement agency" after "Section 626,"; and (2) "or was taken before any officer of a law enforcement agency, or, in any case, at any time after such person has reached the age of 21 years" after "Section 626."

Former § 781, similar to CC § 236, was enacted 1937 and repealed by Stats 1961 ch 1616 § 1 p 3459.

PRACTICE REMINDERS

■ When a minor has been proceeded against in juvenile court for criminal offenses under provisions of this section and not referred to the Youth Authority, he should answer in the affirmative when questioned concerning his arrest when applying for employment, unless his records had been expunged. Since he may reply in the negative if the records have been expunged, counsel may find it desirable to petition for expungement of records under this section.

A petition filed under this section may be submitted over a verification in the form of a certification or declaration made under penalty of perjury in lieu of a sworn statement made under oath.

Collateral References:

Cal Jur 2d Delinquent, Dependent, and Neglected Children §§ 10, 13 et seq.

McKinney's Cal Dig Delinquent, Dependent and Neglected Children § 12.

Am Jur Juvenile Courts and Delinquent, Dependent, and Neglected Children (rev ed §§ 31 et seq., 79).

Trial Techniques:

14 Am Jur Trials p 701 (expungement of records in juvenile court proceedings).

Law Review Articles:

Measures to curtail postadjudication stigma in juvenile court proceedings. 51 CLR 445.

Sealing of juvenile records. 3 Santa Clara Law 119.

Re-evaluation of California juvenile justice as to sealing of records. 19 Hast LJ 99.

Expungement myth. 38 LA Bar B 161.

Wiping out criminal or juvenile record. 40 St BJ 816.

Attorney General's Opinions:

40 Ops Atty Gen 50 (filing, etc. of sealed records of juveniles).

43 Ops Atty Gen 288 (proper answer by applicant for employment to question of whether applicant has ever been arrested where he is or was minor proceeded against in Juvenile Court).

Annotations:

Constitutionality, construction, and application of statutory provision against use in evidence in any other case of records, or evidence in juvenile court proceedings, 147 ALR 443.

TITLE 8. OF JUDGMENT AND EXECUTION

CHAPTER 1. THE JUDGMENT

§ 1203.45 Petition for order sealing records; exceptions

(a) In any case in which a person was under the age of 18 years at the time of commission of a misdemeanor and is eligible for, or has previously received, the relief provided by Section 1203.4 or 1203.4a, such person, in a proceeding under Section 1203.4 or 1203.4a, or a separate proceeding, may petition the court for an order sealing the record of conviction and other official records in the case, including records of arrests resulting in the criminal proceeding and records relating to other offenses charged in the accusatory pleading, whether defendant was acquitted or charges were dismissed. If the court finds that such person was under the age of 18 at the time of the commission of the misdemeanor, and is eligible for relief under Section 1203.4 or 1203.4a or has previously received such relief, it may issue its order granting the relief prayed for. Thereafter such conviction, arrest, or other proceeding shall be deemed not to have occurred, and the petitioner may answer accordingly any question relating to their occurrence.

(b) This section applies to convictions which occurred before, as well as those which occur after, the effective date of this section.

(c) This section shall not apply to offenses for which registration is required under Section 290, to violations of Division 10 (commencing with Section 11000) of the Health and Safety Code, or to misdemeanor violations of the Vehicle Code relating to operation of a vehicle or of any local ordinance relating to operation, standing, stopping, or parking of a motor vehicle.

(d) This section does not apply to a person convicted of more than one offense, whether the second or additional convictions occurred in the same action in which the conviction as to which relief is sought occurred or in another action, except in the following cases:

(1) One of the offenses includes the other or others.

(2) The other conviction or convictions were for the following:

(i) Misdemeanor violations of Chapters 1 (commencing with Section 21000) to 9 (commencing with Section 22500), inclusive, or Chapters 12 (commencing with Section 23100) to 14 (commencing with Section 23340), inclusive, of Division 11 of the Vehicle Code, other than Sections 23101 to 23108, inclusive, or Section 23121.

(ii) Violation of any local ordinance relating to the operation, stopping, standing, or parking of a motor vehicle.

(3) The other conviction or convictions consisted of any combination of paragraphs (1) and (2).

- -

(e) In any action or proceeding based upon defamation, a court, upon a showing of good cause, may order any records sealed under this section to be opened and admitted into evidence. The records shall be confidential and shall be available for inspection only by the court, jury, parties, counsel for the parties, and any other person who is authorized by the court to inspect them. Upon the judgment in the action or proceeding becoming final, the court shall order the records sealed.

(Amended by Stats.1972, c. 579, p. —, § 38.)

§ 851.7 Petition to seal court records by person arrested for misdemeanor while a minor; grounds; exceptions

(a) Any person who has been arrested for a misdemeanor, with or without a warrant, while a minor, may, during or after minority, petition the court in which the proceedings occurred or, if there were no court proceedings, the court in whose jurisdiction the arrest occurred, for an order sealing the records in the case, including any records of arrest and detention, if any of the following occurred:

(1) He was released pursuant to paragraph (1) of subdivision (b) of Section 849.

(2) Proceedings against him were dismissed, or he was discharged, without a conviction.

(3) He was acquitted.

(b) If the court finds that the petitioner is eligible for relief under subdivision (a), it shall issue its order granting the relief prayed for. Thereafter, the arrest, detention, and any further proceedings in the case shall be deemed not to have occurred, and the petitioner may answer accordingly any question relating to their occurrence.

(c) This section applies to arrests and any further proceedings that occurred before, as well as those that occur after, the effective date of this section.

(d) This section does not apply to any person taken into custody pursuant to Section 625 of the Welfare and Institutions Code, or to any case within the scope of Section 781 of the Welfare and Institutions Code, unless, after a finding of unfitness for the juvenile court or otherwise, there were criminal proceedings in the case, not culminating in conviction. If there were criminal proceedings not culminating in conviction, this section shall be applicable to such criminal proceedings if such proceedings are otherwise within the scope of this section.

(e) This section does not apply to arrests for, and any further proceedings relating to, any of the following:

(1) Offenses for which registration is required under Section 290.

(2) Offenses under Division 10 (commencing with Section 11000) of the Health and Safety Code.

(3) Offenses under the Vehicle Code or any local ordinance relating to the operation, stopping, standing, or parking of a vehicle.

(f) In any action or proceeding based upon defamation, a court, upon a showing of good cause, may order any records sealed under this section to be opened and admitted in evidence. The records shall be confidential and shall be available for inspection only by the court, jury, parties, counsel for the parties, and any other person who is authorized by the court to inspect them. Upon the judgment in the action or proceeding become final, the court shall order the records sealed.

(Added by Stats.1967, c. 1373, p. 3223, § 1. Amended by Stats.1970, c. 497, p. 978, § 1.)

Cross References

Petition for order sealing records, see § 1203.45.

§ 2947. Communications intended to deprive discharged prisoner from employment or to extort; threats; offense

Any person who knowingly and wilfully communicates to another, either orally or in writing, any statement concerning any person then or theretofore convicted of a felony, and then finally discharged, and which communication is made with the purpose and intent to deprive said person so convicted of employment, or to prevent him from procuring the same, or with the purpose and intent to extort from him any money or article of value; and any person who threatens to make any said communication with the purpose and intent to extort money or any article of value from said person so convicted of a felony is guilty of a misdemeanor.

(Added by Stats.1941, c. 106, p. 1108, § 15.)

Cross References

Communications intended to deprive parolees from employment or to extort funds, prohibition of, see § 3058.
Definitions,
Felony, see § 17.
Misdemeanor, see § 17.
Punishment for misdemeanor, see §§ 19, 19a.
Threats inducing fear to expose commission of a crime, see § 519.
Use of photograph or fingerprints to detriment of employee or applicant for employment, see Labor Code § 1051.

§ 3058. Communications intended to deprive parolee from employment or to extort; threats; offense

Any person who knowingly and wilfully communicates to another, either orally or in writing, any statement concerning any person then or theretofore convicted of a felony, and then on parole, and which communication is made with the purpose and intent to deprive said person so convicted of employment, or to prevent him from procuring the same, or with the purpose and intent to extort from him any money or article of value; and any person who threatens to make any said communication with the purpose and intent to extort money or any article of value from said person so convicted of a felony, is guilty of a misdemeanor.

(Added by Stats.1941, c. 106, p. 1113, § 15.)

Cross References

Discharged prisoners, similar provision protecting, see § 2947.
Extortion defined, see § 518.
Felony defined, see § 17.
Misdemeanor,
  Defined, see § 17.
  Punishment, see §§ 19, 19a.

PROPOSED CALIFORNIA LAW

The people of the State of California do enact as follows:

SECTION 1. Article 6 (commencing with Section 11140) is added to Chapter 1 of Title 1 of Part 4 of the Penal Code, to read:

Article 6. Unlawful Furnishing of Master Record Sheet

11140. As used in this article:

(a) "Record" means the master record sheet, or a copy thereof, maintained under a person's name by the Department of Justice, and which is commonly known as "arrest record," "criminal record sheet," or "rap sheet." "Record" does not include any other records or files of the Department of Justice.

(b) "A person authorized by law to receive a record" means any person or public agency authorized by *a court order or by* a specific statute of the State of California to receive a ~~record as defined in subdivision (a), or any public agency which, or public officer or official who, needs the information contained in such a record for the performance of an official function.~~ *record.*

11141. Any employee of the Department of Justice who knowingly furnishes a record, or information ~~obtained from a record, to a person whom he knows is not authorized pursuant to law to receive such record or information is guilty of a misdemeanor.~~ *obtained from a record, to a person who is not authorized by law to receive a record or information is guilty of a misdemeanor.*

11142. Any person authorized *by law* to receive a record *, or information obtained from a record,* ~~pursuant to law who knowingly furnishes the record, or~~ *who knowingly furnishes the record, or* information obtained from ~~such~~ *a* record, to a person ~~whom he knows is~~ not authorized by law to receive ~~such~~ *a* record or information is guilty of a misdemeanor.

11143. ~~Every~~ *Any* person who, knowing he is not ~~authorized pursuant to law to receive a record or~~

authorized by law to receive a record or information obtained from ~~such~~ *a* record, ~~buys or receives~~ *knowingly buys, receives, or possesses* ~~such~~ *a* record or information is guilty of a misdemeanor.

11144. (a) It is not a violation of ~~Section 11141 or 11142 to disseminate for statistical or research purposes~~ *this article to disseminate statistical or research* information obtained from a record, provided that the identity of the subject of the record is not disclosed.

(b) It is not a violation of ~~Section 11141 or 11142 for a law enforcement agency~~ *this article* to disseminate information obtained from a record for the purpose of assisting in the apprehension of a person wanted ~~by that agency~~ in connection with the commission of a crime.

SEC. 2. The sum of _____ dollars ($_____) is hereby appropriated from the General Fund to the State Controller for allocation and disbursement to local agencies pursuant to Section 2164.3 of the Revenue and Taxation Code to reimburse such agencies for costs incurred by them pursuant to this act.

CALIFORNIA

DEPARTMENT OF JUSTICE POLICY

RECORD RETENTION CRITERIA

The Record Purging Subcommittee of the Interdivision Committee on Criminal Records recommends that the following record retention criteria be implemented by the Department of Justice.

I. The Bureau of Identification discontinue creating records for certain specified and limited subjects. These include:

a. Subjects arrested for drunk, 647(f) PC, unless the local reporting agency indicates that the arrest was for being under the influence of drugs.

b. Subjects arrested for violation of local ordinance, except for those ordinances falling within classifications of statewide interest which will be developed by a special committee of CPOA by January 10.

c. Subjects arrested for minor traffic offenses. A minor traffic offense is defined as any traffic offense which is not listed in Attachment 1.

d. Subjects arrested for such minor or nonspecific offenses as "investigation," "suspicion," "lodger," "inquiry," or "disorderly," except where specific reference to an offense which is otherwise recordable is provided by the reporting agency. (See attachment 2)

e. Subjects of an applicant clearance request unless submitted by a state agency with whom the department has a contract to provide notification service in the event of a subsequent arrest.

II. The Bureau of Identification discontinue adding to existing records those types of dispositions and reports listed in recommendation I.

III. The Bureau of Identification establish realistic retention periods and develop a purge program. The retention periods are as follows:

a. Zero retention period for arrests and applicant clearances which are referred to in recommendations I and II.

b. A 5-year retention period for misdemeanor arrests not resulting in a conviction, or arrests which are later termed a "detention only" under PC 849(b). The retention period is to begin running on the date of arrest or detention.

c. A 7-year retention period for misdemeanor arrests resulting in a conviction with the retention period commencing at the date of arrest.

d. A 7-year retention period for arrests nor resulting in a conviction for an offense where a prior constitutes a felony, for an offense which would be a felony depending upon disposition, and for felonies. The retention period is to begin running on the date of arrest.

e. A modified lifetime retention period for a conviction of an offense where a prior constitutes a felony, of an offense which would be a felony depending upon disposition, and of a felony. If the subject lives to age 70, and has had no contacts with the criminal justice system since age 60, the record will be purged from Department of Justice files. If the individual has had contact with the criminal justice system after age 60, his record will be maintained for the applicable retention period, or in the case of a felony or similar offense, for a 10-year period commencing with the date of release from supervision.

f. Applicant prints maintained pursuant to a contract with a state agency shall be retained until the contracting agency indicates it is no longer interested in the subject or until the contract is terminated.

Excluded from retention periods will be convictions requiring registration under Penal Code § 290 so long as registration is required.

IV. The Bureau of Identification will arrange with the Department of Health to receive copies of death certificates for the purpose of purging from its files deceased persons. Records on individuals known to be deceased will be maintained for a 3-year period after the individual's date of death.

Attachment 1

Recordable Traffic Offenses

Section #	Code	Description
20	VC	False statements
31	VC	Giving false information to peace officer
480	VC	Hit and run/death or injury
481	VC	Hit and run/property damage
501	VC	Felony drunk/narcotic driving
502	VC	Misdemeanor drunk/narcotic driving
503	VC	Take auto without owner's consent
504	VC	Tamper with auto
506(a)	VC	DUI narcotic drug
506(b)	VC	DUI non-narcotic drug
506.1	VC	DUI dangerous drugs
2261	VC	Impersonating CHP officer
4463	VC	Forge/alter auto registration, etc
Div. 4	VC	Pertaining to theft, including altering/changing vehicle I.D. number, etc.
10850	VC	Taking auto without owner's consent
10851	VC	Taking auto without owner's consent
10852	VC	Tampering with auto
10853	VC	Malicious mischief to auto
10854	VC	Felony tampering with auto

Recordable Traffic Offenses
Page 2

Section #	Code	Description
10855	VC	Embezzlement of rented auto
11500	VC	Dismantling without a permit
11520	VC	Dismantling vehicle without notifying DMV
11700	VC	Dealer, manufacturer, or transporter without license
11711	VC	Fraud
11713	VC	Unlawful acts
11800	VC	Vehicle sales without license
11806	VC	Proscribed activities
14601	VC	Driving with suspended or revoked license
20001	VC	Hit and run/death or injury
20002(a)	VC	Property damage
23101	VC	Felony drunk/narcotic driving
23101.5	VC	DUI Toluene/poison, felony
23102	VC	Misdemeanor drunk driving
23102(a)	VC	Misdemeanor drunk driving
23102(b)	VC	Misdemeanor drunk driving
23102.5	VC	DUI Toluene/poison, misdemeanor
23102.5(a)	VC	DUI Toluene/poison, misdemeanor
23102.5(b)	VC	DUI Toluene/poison, with prior
23103	VC	Reckless driving

Section #	Code	Description
23104	VC	Reckless driving with injury
23105	VC	DUI narcotic drug
23105.5(a)	VC	DUI Toluene/poison, misdemeanor
23106	VC	Non-narcotic drugs, misdemeanor
23108	VC	Non-narcotic drugs, felony
23109	VC	Speed contests
23110(a)	VC	Throwing at vehicles, misdemeanor

Attachment 2

MINOR AND NONSPECIFIC OFFENSES

1. Investigation
2. Suspicion
3. Lodger or sleeper
4. General principles
5. Inquiry
6. Attachment comtempt of court (no charge)
7. Attempt (no charge given)
8. Bench warrant (no charge given)
9. Bond jumping (no charge given)
10. Disorderly
11. Disorderly conduct, DOC, disorderly conduct drunk, etc.
12. Drunk in/about vehicle
13. Fail to identify
14. Juvenile (no charge given)
15. No driver's license
16. No driver's license in possession
17. Order to show cause (no charge given)
18. Possession of alcohol by minor (25662 B&P Code)
19. Trespass

37-583 O - 74 - pt.2 - 36

AMENDED IN SENATE JUNE 27, 1974
AMENDED IN SENATE JUNE 6, 1974
AMENDED IN ASSEMBLY JANUARY 29, 1974
AMENDED IN ASSEMBLY JANUARY 10, 1974
AMENDED IN ASSEMBLY JANUARY 7, 1974

CALIFORNIA LEGISLATURE—1973–74 REGULAR SESSION

ASSEMBLY BILL No. 2656

Introduced by Assemblymen Bagley, Antonovich, and Chappie
(Coauthor: Senator Marks)

August 31, 1973

REFERRED TO COMMITTEE ON EFFICIENCY AND COST CONTROL

An act to add Title 1.8 (commencing with Section 1798) to Part 4 of Division 3 of the Civil Code, relating to personal data, and making an appropriation therefor.

LEGISLATIVE COUNSEL'S DIGEST

AB 2656, as amended, Bagley (E.C.C.). Personal data.

Imposes safeguards, restrictions, and other specified requirements upon the use and transfer of personal data used by computers in automated personal data systems. Makes it a misdemeanor to fail to conform to certain requirements regarding supplying written notice of the described rights of persons to whom the data pertain.

Requires ~~persons~~ *governmental bodies* maintaining automated personal data systems to file annual notice with Department of Consumer Affairs specifying, among other things,

the nature and purpose of the system and describing intended use thereof. Provides civil penalty for failure to file required report.

Provides cause of action for damages or for an injunction against responsible ~~person~~ *parties, as specified* for noncompliance with the act.

Excludes certain public records from application of the act.

Determines that no relevant evidence relating to any procedure established or required by the act is to be privileged in any civil action for evidentiary purposes, including discovery procedures or other aspects of any cause of action.

Appropriates $4,900,000 to the State Controller for allocation and disbursement to local agencies for costs incurred by them pursuant to this act.

Vote: ⅔. Appropriation: yes. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. Title 1.8 (commencing with Section 1798) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.8. CALIFORNIA FAIR INFORMATION PRACTICE ACT OF 1974

CHAPTER 1. GENERAL PROVISIONS

1798. This act shall be known and may be cited as the California Fair Information Practice Act of 1974.

1798a. Recognizing that the people of California have made clear their desire that their privacy be protected by establishing a constitutional right of privacy, and that the application of computer technology to personal recordkeeping has created new opportunities for invasion of that right of privacy, and that personal privacy is poorly protected in law against abusive recordkeeping practices, and that the power of individuals to affect recordkeeping systems is far weaker than the power of such systems to affect their lives, the Legislature of the

State of California hereby finds and declares that the constitutional right of privacy includes the right of an individual to control the uses made of personal data about him.

Accordingly, the Legislature recognizes these basic principles of fair information practice:

(1) There must be no personal data recordkeeping systems whose very existence is secret.

(2) There must be a way for an individual to find out what personal information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent personal information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

(4) There must be a way for an individual to correct or amend a record of identifiable personal information about him.

(5) An organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

This title shall be construed liberally and in accordance with the principles and findings here set forth.

1798.1. As used in this title:

(a) "Personal data" means any information that describes anything about an individual and which can be associated with an identifiable individual.

(b) "Computer accessible" means recorded on any medium actually used for the storage of data in a form capable of direct use with electronic data processing equipment. "Computer-accessible" media include but are not limited to: (1) magnetic tape, magnetic disk, magnetic drum, punched card, paper tape, or any other magnetic medium; or (2) optically scannable paper or film when these are actually used with optical scanning devices.

(c) "Personal data base" means a set of personal data stored in computer-accessible form.

(d) "Automated personal data system" means a

personal data base used with electronic data-processing equipment and programming.

(e) "Administrative decision" means a determination regarding the qualifications, character, rights, opportunities or benefits of an individual.

(f) "Data subject" means an individual who is the subject of a record in an automated personal data system.

(g) "Department" means the Department of Consumer Affairs.

(h) "Individual" means a natural person.

(i) "Local public entity" means a county, city, district, public authority, public agency, and any other political subdivision or public corporation in the state, but does not include the state.

~~(j) "Person" means an individual, partnership, corporation, association, local public entity, the state, or other group, however organized but not the United States or any agency thereof.~~

(j) "Governmental body" means the state or any local public entity.

(k) "State" means the state and any office, officer, department, division, bureau, board, commission, or agency of the state.

CHAPTER 2. SAFEGUARD REQUIREMENTS FOR AUTOMATED PERSONAL DATA SYSTEMS

1798.2. Every ~~person~~ *governmental body* maintaining an automated personal data system within California shall:

(a) Identify one individual responsible for receiving and responding to (1) inquiries and complaints regarding the system, (2) requests for data pursuant to subdivision (b) of Section 1798.5, and (3) disputes regarding the accuracy, completeness, timeliness, or pertinence of data under subdivision (e) of Section 1798.5.

(b) Exercise due care to ensure that each of its employees is aware of the requirements of this title and of each rule or procedure which may be adopted by the ~~person~~ *governmental body* to ensure compliance with it.

(c) Take no disciplinary or punitive action against any person who in good faith brings to the attention of any ~~person~~ *governmental body* evidence of any violation of this title.

(d) Specify and apply disciplinary measures to be applied to any employee who willfully initiates or otherwise contributes to any disciplinary or other punitive action against any person who brings to the attention of any ~~person~~ *governmental body*, evidence of any violation of this title.

~~(e) Take reasonable care to protect personal data in the system from any release, transfer, access, or use which is in violation of any provision of this title.~~

~~(f)~~ *(e)* Establish and adhere to procedures to ensure that personal data in the system are accurate, complete, timely, and pertinent. Liability for damages under subdivision (a) of Section 1799, in an action brought for violation of this section, shall be limited to cases in which the ~~person~~ *governmental body* maintaining the system did not exercise reasonable care in establishing and adhering to such procedures.

1798.4. (a) Every ~~person~~ *governmental body* maintaining an automated personal data system in California on December 31, 1975, shall give notice of the existence and character of its system prior to January 31, 1976. Such notice shall be filed with the Director of Consumer Affairs and shall be a permanent public record. Every state or local criminal justice agency maintaining an automated personal data system which contains criminal investigatory, intelligence, or security information, shall file a copy of its public notice with the Attorney General *and with the Director of Consumer Affairs*. The director may establish regulations prescribing the form of such notice. The director may charge a yearly filing fee for each notice filed to defray any administrative costs incurred pursuant to this section. Any ~~person~~ *governmental body* maintaining more than one system shall file notices for each such system simultaneously, and such notices may be combined when convenient and appropriate. Any ~~person~~ *governmental*

body who establishes or modifies a system after the effective date of this section shall file a notice as required by this section within 30 days of such establishment or modification. For the purposes of this section, a system is modified when the system as changed would require a different statement on any of the points of the public notice than in the statement as made in the public notice as last previously amended. After a public notice regarding a system has been filed, it must be refiled annually. Such refiling may be made by a letter certifying that the public notice as last amended accurately reflects the current status of the system. The notice shall specify each of the following:

(1) The name of the system. The system name shall be reasonably related to the nature and purpose of the system.

(2) The general nature and purpose of the system and whether or not the data in the system is a public record.

(3) The general type and approximate number of individuals on whom data is to be maintained.

(4) The data elements to be maintained.

(5) A general description of the uses to be made of data in the system, so far as known.

(6) The classes of sources of personal data. The notice shall state whether data is gathered directly from the data subject, from third parties, from public records, or by other specified means.

(7) The title, name, business address and telephone number of the individual specified in subdivision (a) of Section 1798.2

(b) The director shall, each year, compile a list of ~~an~~ automated personal data systems which have filed public notices. For each system, he shall list the contents of public notice required by paragraphs (1), (2), and (7) of subdivision (a) ~~of Section 1798.1~~. The director shall cause this list to be printed under the title "The Citizen's Guide to Automated Personal Data Files", and he shall have such list distributed to state*, county, and city* libraries, and to any other ~~depository~~ *depositories* he deems appropriate.

(c) Notwithstanding any other provision of this title, every ~~person~~ *governmental body* who willfully fails to file a notice as required by this section shall be liable for a civil penalty not to exceed ten thousand dollars ($10,000) for each violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General or by any district attorney in any court of competent jurisdiction. If brought by the Attorney General, one-half of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered, and one-half to the State Treasurer. If brought by a district attorney, the entire amount of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered.

CHAPTER 3. RIGHTS OF DATA SUBJECTS

1798.5. Every ~~person~~ *governmental body* maintaining an automated personal data system in California shall do each of the following:

(a) Clearly and conspicuously disclose to an individual asked to supply personal data about himself to the system, at the time he is asked to supply the data, (1) the general purpose for which the data is requested, and (2) whether the data requested is required by law, or by administrative regulation, or is optional. The general purpose disclosed to the individual under this section shall be substantially similar to the purpose stated in the public notice under paragraph (2) of subdivision (a) of Section 1798.4. If the data will become a public record under Sections 6250 through 6260 of the Government Code, or any similar provisions, disclosure of the purpose for which data is requested shall include disclosure of the fact that the data will become a public record. If the data requested may become part of an automated personal data system, but will not routinely become part of a system in the ordinary course of business, no disclosure shall be required under this section.

(b) Inform in writing an individual, upon his request

and proper identification, whether he is the subject of data in the system, and if so, make such data fully available to the individual in a form comprehensible to him. The ~~person~~ *governmental body* may impose a charge for such reports reasonably related to cost and not to exceed five dollars ($5). Such reports shall be made within a reasonable time from the receipt of the request, not to exceed six weeks.

The ~~person~~ *governmental body* maintaining the system may use a printout of data in the system for the purpose of informing individuals as required by this section, rather than retrieving data separately for each request. If the ~~person~~ *governmental body* chooses to maintain a printout for this purpose, the ~~person~~ *governmental body* must establish procedures to ensure that the printout is updated in a timely manner to reflect changes in data in the system.

(c) Ensure that no *release, transfer, access, or* use of individually identifiable personal data is made that is not consistent with the stated purposes of the system as reasonably understood by the individual from the information provided him pursuant to subdivision (a) of this section when such information has been provided, unless the prior informed consent of the individual has been explicitly obtained; and ensure, when personal data is gathered from sources other than the data subject, that no use of individually identifiable personal data is made that is not consistent with the stated purposes of the system as would be reasonably understood from the notice required by paragraph (2) of subdivision (a) of Section 1798.4, unless the prior informed consent of the individual has been explicitly obtained. Personal data may be transferred from one system to another without the prior informed consent of an individual, if the purpose for which the receiving ~~person~~ *governmental body* will use the data, as disclosed in the public notice required by paragraph (2) of subdivision (a) of Section 1798.4 is substantially the same as that of the transferring person. Data may also be disclosed to federal, state, or local government when such disclosure is authorized or

required by law. Data which has been obtained solely from a public record may be used for any purpose and transferred to any ~~person~~ *governmental body* without the prior informed consent of the data subject. No ~~person~~ *governmental body* shall be held liable for a violation of this section if he shows by a preponderance of the evidence that at the time of the alleged violation he maintained reasonable procedures to ensure compliance with it.

(d) Ensure that no data about an individual other than name and address are made available from the system in response to a demand for data made by means of compulsory legal process, unless a reasonable effort has been made to notify the individual to whom the data pertain of the demand.

(e) Maintain procedures that allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and timeliness.

(f) If the accuracy, completeness, pertinence, or timeliness of personal data is disputed, and such dispute is directly conveyed to the ~~person~~ *governmental body* maintaining the personal data, the ~~person~~ *governmental body* shall reinvestigate and record the current status of that personal data. If, after such reinvestigation it is found that personal data is not accurate, complete, pertinent, or timely, or that the data can no longer be verified, the ~~person~~ *governmental body* shall correct or delete such personal data.

If the ~~person~~ *governmental body* maintaining the system and the data subject fail to resolve their dispute after reinvestigation of the data, the dispute may be resolved in one of three ways to be elected by the ~~person~~ *governmental body* maintaining the system: ~~(1)~~ ~~the~~ *(1) The* data subject may file with the ~~person~~ *governmental body* maintaining the system a brief statement setting forth his views on the dispute. The ~~person~~ *governmental body* maintaining the system may limit the statement to 100 words if the statement is stored in computer-accessible form, or to one page if it is stored in computer associated or referenced form, provided, in

either case, that the ~~person~~ *governmental body* provide the data subject with assistance in writing a clear and accurate summary of the ~~dispute.~~

~~Whenever a statement of a dispute is filed, the person~~ *dispute. Whenever a statement of dispute is filed, the governmental body* maintaining the system shall, in any subsequent disclosure or dissemination of the disputed data, clearly note that it is disputed by the data subject and provide with the data either a copy of his statement or a clear and accurate summary thereof. ~~(2) The parties to the dispute~~ *(2) The parties to the dispute* may agree to binding arbitration of the dispute. ~~(3) The~~ *(3) The* data subject may seek injunctive relief ordering the ~~person~~ *governmental body* maintaining the data to amend, correct, or purge the disputed data.

This section shall not be construed to supersede any remedy available to a data subject by law. This section shall not apply in any case in which a procedure for resolving disputes is provided by law, nor in cases in which the data is determined by a final court order or judgment. This subdivision shall not apply to any sworn public record for which an amendatory procedure is provided by law.

Chapter 4. Remedies and Procedures

1799. (a) Any ~~person~~ *governmental body* who violates any provision of this title is liable to any person who suffers any damage as a result of such violation, and the person damaged may bring an action against such other ~~person~~ *governmental body* to recover any damages sustained.

(b) Any ~~person~~ *governmental body* who willfully or maliciously violates any provision of this title shall be subject to such punitive damages as the court may allow.

(c) Any ~~person~~ *governmental body* who willfully or maliciously violates any provision of this title shall be liable to any person who suffers any damage as a result of such violation for treble actual damages sustained.

(d) Any ~~person~~ *governmental body* who knowingly

and willfully obtains or uses, or attempts to obtain or use, personal data, and who is not authorized to use such data under subdivision (c) of Section 1798.5, shall be fined not more than five thousand dollars ($5,000) or imprisoned not more than one year, or both.

(e) Any ~~person, or employee of a person~~ *governmental body, or employee of a governmental body*, maintaining an automated personal data system, who knowingly and willfully provides personal data from the system to a ~~person~~ *governmental body* in violation of this title shall be fined not more than five thousand dollars ($5,000) or imprisoned for not more than one year, or both.

(f) Any ~~person who~~ *governmental body that* violates or proposes to violate this title may be enjoined by any court of competent jurisdiction. The court may make such order or judgment, as may be necessary to prevent the use or employment by any ~~person~~ *governmental body* of any practices which violate this title.

Actions for injunction under this subdivision may be prosecuted by the Attorney General or any district attorney in this state in the name of the people of the State of California upon their own complaint or upon the complaint of any ~~person~~ *governmental body* acting for the interests of itself, its members or the general public, or of any individual acting in his own behalf.

(g) Any action filed pursuant to this title may be commenced in the county in which the individual or person alleging damage or seeking relief resides, or in the county in which the ~~person against whom it is brought resides, has his principal place of business, or is doing business.~~ *governmental body is situated.*

(h) An individual entitled to bring an action under any provision of this title may, if the alleged violation has caused or may cause damage to other individuals similarly situated, bring an action on behalf of himself and such other individuals to recover damages or obtain relief as provided in this title. Any action pursuant to this subdivision shall be governed by the rules prescribed in subdivisions (b) to (g), inclusive, of Section 1781.

(i) In the case of any successful action under the provisions of this title, the defendant shall be liable for the costs of the action together with reasonable attorney's fees as determined by the court.

1799.1. No relevant evidence, relating to any procedure established or required by this act shall be privileged in any action for evidentiary purposes, including but not limited to, discovery procedures or other aspects of any cause of action.

1799.2. ~~This~~ *(a) This* title shall not limit in any way the operation of the Public Records Act found in Sections 6250 to 6260, *inclusive,* of the Government Code. Any record of personal data which by law is a matter of public record shall remain a public record. This title shall not require disclosure of any record to any individual, if by law it may not be disclosed to the individual. This title shall not limit in any way the transfer, access, or use of personal data when such transfer, access, or use is permitted or required by law.

(b) Nothing in this title shall require disclosure to a data subject of any information exempt from public disclosure by Section 6254(f) of the Government Code. Nothing in this title shall require the disclosure to a data subject of medical or psychiatric records. Nothing in this title shall prohibit the transfer of medical data for the purpose of processing insurance claims.

SEC. 2. The Intergovernmental Board on Electronic Data Processing shall study the effects of this title and on April 1, 1976, and April 1, 1977, transmit a report of its findings to a committee to be composed of the Commissioner of Corporations, the Commissioner of Banking, the Insurance Commissioner, the Attorney General, the Commissioner of Savings and Loans, and the State Controller as chairman, or their representatives.. This committee shall study the report of the Intergovernmental Board on Electronic Data Processing and transmit that report and the committee's findings and recommendations for further legislation in the area of personal data privacy and fair information practice to the Legislature before June 1, 1976, and June 1, 1977.

SEC. 3. The sum of four million nine hundred thousand dollars ($4,900,000) is hereby appropriated from the General Fund to the State Controller for allocation and disbursement to local agencies pursuant to Section 2231 of the Revenue and Taxation Code to reimburse such agencies for costs incurred by them pursuant to this act.

STATE OF CONNECTICUT

EXECUTIVE CHAMBERS,
HARTFORD,
August 30, 1974.

Hon. SAM J. ERVIN, Jr.
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: In your letter of June 25, 1974, you asked for my comments upon the desirability and practicability of proposed Senate Bill 3418. On July 9, 1974, I stated that I had asked my staff to research the subject for me. Having received this staff work, I am now forwarding my comments to you.

The subject of privacy is of vital interest to the citizens of Connecticut, affecting many aspects of everyday life. For example, the proposed bill would have a direct impact on several agencies of state government. The Connecticut Tax Department, and the Connecticut Council on Human Services would have to alter their policies relating to confidentiality. The bill would also have a significant impact on the design of the proposed Connecticut Criminal Justice Information System, and the selection and location of the computer "hardware" associated with it.

In the private sector, many Connecticut corporations, principally insurance companies and banks, have great interest in the subject of privacy since modifications in their record keeping and information gathering systems would be required under the new system.

ANALYSIS AND RECOMMENDATIONS

The scope of S. 3418 is extremely broad. Establishing standards of operation for citizen-oriented information systems both in the private and public sectors under a controlling organization appears to be the most sensible approach yet recommended. Because of known abuses of confidentiality, previous bills have been targeted at specific types of information and the systems that generate this information. S. 3418, however, focuses on the constraining factors necessary to insure the confidentiality of *all* personal information and, therefore, the privacy of each individual regardless of the system used (except for those systems exempted), by defining the criteria of privacy and security under which any records system can operate.

TITLE I

Unfortunately, the inherent strength of this bill—the establishment of minimum standards with a body for controlling their implementation—may also be a mechanism for its limited usefulness and, therefore, the subjugation of its purpose.

The further definition of standards and the establishment of the criteria necessary to detail the severity or specificity under which systems will be required to operate is the responsibility of the Federal Privacy Board. An unknowledgeable or lenient board could allow the definition of operating criteria to be stated in broad terms, perpetrating systems which violate the intent of the Bill.

In addition, states which have a more severe or restrictive policy on privacy and security, and which might already meet the intent of the Bill, may not be allowed to implement their provisions because of the requirement that the Board has the right to delegate and, therefore, also withhold delegation of their powers to that state.

Thus, in these two instances, it is not the *bill* that jeopardizes the privacy of the individual but the *Board* designated as responsible for its implementation.

Since it appears that the intent of the Bill is to set *national* standards of privacy and to provide direction to the individual states for establishing their own laws, the inclusion of a statement as made in S. 3633, Section 12—Precedence of Other Federal and State Laws—might help to control the activities of the Board as well as dictate a level of severity to which the Board must also comply. This, in effect, would make "watchdogs" of those states which take seriously their responsibility to protect the right to privacy of their citizenry. Section 12 of S. 3633 cited above states:

"Any Federal or State Law, or regulation which places greater restrictions upon the dissemination of personal information or the operation of personal in-

formation systems or which affords to any indivduals, whether juveniles or adults, rights of privacy or protections greater than set forth in this Act shall take precedence over this Act."

This provision would serve to strengthen the Bill.

Third, the Bill requires the Board to publish annually a Date Base Directory containing the name and characteristics of each personal information system. The intent of this requirement and other requirements within Title II for the public notice of personal information systems is to meet the HEW recommended *Code of Fair nformation Practice* provisions which state:

"There must be no secret personal data record-keeping systems;" and "There must be no personal data record-keeping systems whose existence is secret."

This, of course, is a most important part of the overall thrust of this proposed legislation.

TITLE II

The exemptions (Section 202) identify three types of systems which are not required to comply with any provisions as this Title. This is an implication that these systems are responsible to the Federal Privacy Board, but this is not specifically required in Title I. This requirement should be clarified. These types of systems should meet most if not all of the standards as defined in title II. While the rights of the citizenry to have access to specific information about themselves *under certain circumstances* may be negotiable, it should be known, at the least, that the systems exist and that they do meet the standards of operation required by this Bill. Since this Bill appears to exempt the three types of systems from any standard of privacy and security in their operation, there should be a way of insuring confidentiality and maintaining a person's basic rights without jeopardizing the utility of these types of systems.

On a positive note, the several requirements for notification and access as stated in Section 201, para. (2) item (5) and para's. (c), (d), and (e), while harsh with respect to the operation of any records-keeping system because of the additional tasks they impose, place the burden of responsibility on the system and not on the individual. I believe that this is as it should be. These requirements might have an ancillary benefit of limiting the types of information collected by a system, accruing additional measures of privacy and security, and limiting the potential for abuse by or within any one system.

TITLE III

The criminal penalties and civil remedies stated within Title III hold the organization or the responsible officer of the organization directly accountable for any abuses that occur. This Bill recognizes that privacy and security must be a top management responsibility.

Finally, the effective date of the Bill is to be one year after its enactment, which may be rather severe on many records-keeping operations, forcing their non-compliance of the Act and/or their discontinuance of operation. A staggered implementation of the various sections of this Bill would probably provide an orderly transaction.

I am pleased to have had the opportunity to review and comment upon this legislation. I sincerely hope my comments prove to be helpful to you.

With best wishes,

Sincerely,

TOM MESKILL, *Governor.*

STATE OF FLORIDA

DEPARTMENT OF LEGAL AFFAIRS,
OFFICE OF THE ATTORNEY GENERAL,
Tallahassee, Fla., July 23, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Governmental Operations,
U.S. Senate, Washington, D.C.

DEAR CHAIRMAN ERVIN: Thank you for your recent correspondence forwarding to us a copy of Senate Bill 3418.

We appreciate having the opportunity to review this proposed legislation. We are of the opinion that there is a need for appropriate federal action in this area. Senate Bill 3418 seems to serve as a good vehicle for protecting the in-

dividual's right to privacy. Our only concern, which seems to be covered in the bill, is that it would not curtail the necessary development of information systems for law enforcement agencies.

Though the State of Florida does not currently have any statutory provisions comparable to Senate Bill 3418, this past Legislative session witnessed the passage of certain measures relevant to the individuals right to privacy and the collection of information. Committee substitute for House Bill 3740 revising the Florida Department of Law Enforcement included a provision for the creation of a Division of Criminal Justice Information System. The purpose of the Division is to collect and disseminate information on persons involved in criminal activity. The bill also provides for the creation of a criminal justice information council which would serve to oversee the collection and dissemination of this information to insure that unauthorized or inappropriate disclosure is prohibited. Further, during this legislative session two measures were passed relating to the security of communications specifying certain provisions to insure the individual's right to privacy.

We hope this information has been of assistance to you. We believe Senate Bill 3418 would serve an important and useful function and we are hopeful that it will receive favorable approval.

Sincerely,

ROBERT L. SHEVIN,
Attorney General.

STATE OF FLORIDA,
OFFICE OF GOVERNOR REUBIN O'D. ASKEW,
September 4, 1974.

Honorable SAM J. ERVIN, Jr.,
U.S. Senator, Senate Office Building,
Washington, D.C.

DEAR SENATOR ERVIN: Thank you for the opportunity to review the legislation providing for regulation of personal information systems and the establishment of a Federal Privacy Board. My staff has reviewed the draft and advised me of its content.

The protection of individual privacy through the regulation of personal information systems merits high priority among those issues facing Congress. We are all too aware of the widespread manufacture of such systems and the frequent abuse that evolves out of their distribution.

The proposed legislation is complete as it relates to all levels of government and the private sector. However, there are some areas over which I express concern. There is a need for increased individual protection in cases where disputed data cannot be resolved. The citizen is presented with the single recourse of assistance from the Federal Privacy Board. There is a need for more detailed citizen determination regarding dissemination of his personal file to other information systems. The section dealing with exemptons should be expanded to categorically define and safeguard the rights of all individuals, including criminal offenders.

I feel your committee has made substantial headway toward development of effective legislation dealing with personal information systems. If this office can be of further service in this endeavor, do not hesitate to contact me.

With warm personal regards,

Sincerely,

REUBIN ASKEW, *Governor.*

STATE OF GEORGIA

EXECUTIVE DEPARTMENT,
Atlanta, Ga., July 2, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations, U.S. Senate,
Washington, D.C.

DEAR SENATOR ERVIN: I share your concern for the people of this country whose right of privacy is being abused by the irresponsible management of both public and private information systems. State and local government needs, as well as the needs of Congress, must be met. I believe as you do that these needs can be met without an irrelevant invasion of the citizen's right of privacy.

I appreciate the opportunity you have extended me on behalf of the Committee.

Sincerely,

JIMMY CARTER.

STATE OF ILLINOIS

OFFICE OF THE GOVERNOR,
Springfield, Ill., July 19, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: Thank you for soliciting my opinions regarding the pending privacy legislation.

I too am concerned with the growing threat to individual privacy that we have seen over the last few years.

Our aim in Illinois is to address this problem at the state level where we have noticed the increasing tendency by both government and business to maintain detailed records on the personal lives of our citizens. I have appointed a Commission on Individual Liberty and Personal Privacy to recommend legislative and administrative reforms.

I am confident that government at both the state and federal level can reverse the recent trend which we have all viewed with concern. Your leadership at the national level will go a long way toward beginning this process.

Sincerely,

DAN WALKER.

STATE OF KANSAS

OFFICE OF THE ATTORNEY GENERAL,
Topeka, Kans., July 7, 1974.

Hon. SAM J. ERVIN, Jr.,
U.S. Senator, Chairman,
Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: Thank you for your letter of June 25, 1974, and the enclosures, including the text of S. 3418. The problems which the proposed bill seeks to address are indeed massive and complex. The practicability of any proposed legislation to deal adequately with the problems of privacy is, of course, always open to question.

In response to your letter, I would offer only a few observations on matters which your Committee will doubtless be considering in the future.

The placement of the Board in the scheme of the federal government is a delicate question. Its task, in important part, is to assist the individual citizen in protecting his privacy from encroachments by other agencies of the government, federal and state. In effect, the citizen is called upon to look to one governmental agency to intercede in his behalf with another governmental agency, to assure that his rights to privacy are not abused by that other agency. I can only suggest that consideration be given to a more elaborate description of the relationship between the proposed Board and other federal agencies which maintain information systems.

Section 202 provides for exemptions from the act. Under the first provision thereof, the act does not apply to any information system maintained by a federal agency when the head of that agency determines that the release of the information would seriously damage national defense. This is a broad and ambiguous exemption which is made dependent upon the unilateral determination of the agency head. I suggest that this determination should be made reviewable by the Board itself.

Further, concerning the Board, the act provides that the term of each member shall be three years. I question whether this is long enough to permit the Board to establish the necessary independence and continuity it will require to deal adequately with the varied and complex problems in this area.

Under section 103(3), the Board is empowered to delegate its authority to any state, with respect to information systems within the state, when the Board

is satisfied that the state-established authority is carrying out the provisions and requirements of the act. Without additional incentives, few states will be encouraged to undertake this responsibility. In Kansas, to my knowledge, there has been no active legislative interest in these serious questions concerning privacy, save for enactment of the Fair Credit Reporting Act, as part of the Uniform Consumer Credit Act, enacted in 1973. I believe that the states should be encouraged to assume responsibility in this area, and that consideration should be given to providing additional incentives, perhaps in the conventional mold of financial assistance, contingent upon assumption of responsibility in this area. States thus may be free to develop standards and requirements which may be more strict, in many instances, than those adopted federally.

Unfortunately, time does not permit me to dwell at greater length on the many questions which deserve to be explored here. I hope that these few brief observations will be helpful to you and the Committee.

Yours very truly,

VERN MILLER,
Attorney General.

STATE OF KENTUCKY

OFFICE OF THE GOVERNOR,
Frankfort, Ky., August 13, 1974.

DEAR SAM: As mentioned in my July 2nd letter, I have forwarded S3418 to our Department of Justice for comments. I am enclosing a copy of the memoranda received from the Department. I trust that you will understand that the Department's comments relate to practical application, and that they are made from the viewpoint of an agency whose mission is law enforcement and rehabilitation.

Sincerely,

WENDELL FORD.

COMMONWEALTH OF KENTUCKY,
DEPARTMENT OF JUSTICE,
Frankfort, Ky., July 26, 1974.

Mr. EDWIN A. LOGAN,
Legal Assistant to the Governor, Office of the Governor, New Capitol Building, Frankfort, Ky.

DEAR ED: On July 2, 1974 Governor Ford forwarded to me (and to Secretary Pryor) a copy of correspondence and pertinent proposed legislation sent to him by Senator Ervin concerning privacy and security of information stored in data systems. The Governor requested an analysis of the legislation as it might affect data systems operated by the Commonwealth.

The applicable system in the Department of Justice is presently operated by the Bureau of State Police. For that reason I sought the advice of Commissioner Ron Johnson who sent me the enclosed memorandum noting objectionable features of the legislation with respect to criminal justice data systems.

It would seem to me additional questions might be raised about the proper applicability of this legislation when a full criminal justice information system is in being. Would then a court, a corrections agency or similar entity be a law enforcement agency exempt from the legislation, and what effect would the period "necessary to commence criminal prosecution" provision have upon the legitimate needs of the judge, the warden, the parole board and the parole supervision personnel for pertinent information about a person involuntarily coming before them?

We have made no attempt to evaluate non-criminal justice types of data systems in Kentucky operated or maintained by Finance, Revenue, licensing agencies, etc., since their needs are outside the jurisdiction of the Department of Justice.

If you desire further information, please advise.

Sincerely yours,

HENRI MANGEOT,
Secretary, Department of Justice.

Enclosure (1).

To: Secretary Mangeot.
Subject: S. 3418—Federal Privacy Act.
From: Commissioner Johnson.

Although virtually everyone will agree that additional safeguards are needed to protect the right of privacy of all citizens from further encroachment made possible by the almost unlimited storage and access of personal data by computer data systems, several portions of the proposed Act would make it impossible for police agencies to maintain any semblance of a functional criminal records system, criminal history file or criminal intelligence file.

Under the Exemptions, Sec. 202(2), law enforcement agencies are excluded from the provisions of the Act except "where such files have been maintained for a period longer than is necessary to commence criminal prosecution,"———

The exemption appears to be limited to "active criminal investigatory files" and is further limited by the time period "necessary to commerce criminal prosecution" as set out above.

This would appear to rule out keeping records of criminal convictions once a person has been prosecuted, records of known or suspected narcotics pushers unless a criminal prosecution could be instituted within a time that was considered reasonable by the Federal Privacy Board and criminal intelligence files could not be maintained on individuals know to be affiliated with organized criminal operations.

The notice provisions under Sec. 201 requires each organization maintaining a personal information system to notify by mail each data subject at their last known address of the type of information held in such system, expected uses allowed or contemplated, and provide the name and full address of the place where the data subject may obtain personal information pertaining to him in the system. This provision would make it impossible for law enforcement agencies, motor vehicle departments and other governmental agencies who are charged with the responsibility of keeping records to perform any type of necessary function.

Sec. 203 prohibits any organization from requiring a person to furnish his social security number for any purpose in connection with any business or commercial transaction.

It is difficult to visualize how this information would result in an invasion of privacy. It will result in a limited effect in criminal cases involving the forging and cashing of checks as bussinesses who cash checks will no longer be permitted to require the endorser to exhibit his social security card. Probably the most detrimental aspect of this provision will be the inability of older persons who have no driver's license or acceptable identification, other than a social security card, to cash their social security or other checks at business establishments where they are not well known.

The total effect of the proposed bill on all types of governmental agencies would seem to need much more study before it is passed into law.

In the absence of any effective legislation to safeguard the right of privacy of persons who are the subject of data in the criminal files of the Kentucky State Police, more stringent guidelines on the release of criminal record information were recently adopted which are set forth in Exhibit A attached hereto.

RON L. JOHNSON, *Commissioner.*

Attachment.

OFFICE OF THE COMMISSIONER,
KENTUCKY STATE POLICE
Frankfort, Ky., March 22, 1974.

To: All supervisory personnel.
From: Commissioner Ron Johnson.

Effective immediately, it will be the policy of this bureau that criminal records, arrest records and other records regarding proven or suspected criminal offenses *shall not be made available to any* individual or entity, with the following exceptions:

1. Recognized law enforcement agencies or their official representatives or employees.

2. Individuals who are proven to be the subjects of criminal history or arrest record files (viewing or copying shall be limited to the subject's file only and corrections shall be made upon verification of any error in subject's file.)

3. Appropriate information regarding criminal cases may be made available to recognized criminal justice agencies or offices upon approval of either the Commander or Commissioner of State Police.

This directive in no way shall affect present guidelines for officers' *statements* of fact regarding *current* cases, or the dissemination of statistical information.

This policy is necessary to assure that the Kentucky State Police protects the rights of privacy of all citizens until more specific guidelines are established by the courts or legislative bodies.

This policy shall remain in effect until rescinded or amended by the Commissioner of State Police.

STATE OF LOUISIANA

EXECUTIVE DEPARTMENT,
Baton Rouge, La., July 22, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: Thank you so much for your letter on Senate Bill S. 3418 about the management information systems. I share your views on this subject and offer any assistance you might need from our State.

With warmest personal regards.

Sincerely,

EDWIN EDWARDS.

STATE OF LOUISIANA,
DEPARTMENT OF JUSTICE,
Baton Rouge, September 7, 1974.

Re S.B. 3418 Information Systems.

HON. SAM J. ERVIN, Jr.,
U.S. Senator, Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: I have and thank you for your letter of June 25, 1974 requesting my views on pending federal legislation regarding the matters of privacy and security of information about people.

At the present time the only positive action being taken in Louisiana on matters of privacy and security is in the area of criminal offender record information. I am attaching our regulations and comments regarding privacy for your perusal.

A law which will safeguard information about people in general has been needed for a long time. The advent of the computer age and the apparent misuse of data throughout this nation makes evident the pressing need for such legislation.

I am still reviewing S.B. 3418 and hope to have additional comments to make regarding it in the not too distant future, I do feel however, that our productive citizens should be afforded at least the same protection as that of our criminal element.

Very truly yours,

WILLIAM J. GUSTE, Jr.,
Attorney General of Louisiana.

Enclosures.

LCJIS COMMENTS ON PRIVACY & SECURITY ISSUES

NEED FOR FEDERAL LEGISLATION

Many states including Louisiana presently are actively considering Privacy/Security legislation. The bills currently under consideration in the states take many forms and propose varying approaches to the problems. There is a need for a federal law to assure some degree of uniformity in the laws of the states and to settle some of the uncretainty that now exists as to what will be required or permitted in the way of state action to implement security and privacy safeguards, and what standards new state and local systems will have to meet.

Some of the states that now have or are working on legislation to protect personal privacy from potential abuses of automated systems are concerned when their information is disseminated to other states without proper safeguards. Hopefully, federal legislation will provide the catalyst that will spur all of the states to prompt action so that uniform safeguards will exist throughout the Nation.

With respect to the form that such federal legislation should take, there are several important points that should be kept in mind. First is the overriding need of the criminal justice system for information—information that is timely, accurate and responsive to the needs of the various components of the criminal justice community. Numerous studies, beginning with the 1967 Report of the President's Commission on Law Enforcement and Administration of Justice and continuing through the Report of the National Advisory Commission on Criminal Justice Standards and Goals released last year by LEAA, have documented the heavy dependence of the criminal justice system on information about how the system works and about the people involved in the system.

Before stopping a suspicious vehicle, a police officer should know whether it is stolen, who the owner is and whether he is wanted by the police or has a criminal record that might indicate that he is dangerous. Before admitting a defendant to bail, a magistrate should have information about his background and previous criminal record, if any. Before sentencing a convicted offender, a judge should have information about his criminal background. The same kind of information should be available to correction officials considering whether or not to release an offender on parole.

Until relatively recently, criminal justice information systems were, in most cases, inadequate to meet these operational needs of criminal justice agencies. Moreover, as we are sure the officials at LEAA will agree, lack of sufficient information about the operation of the criminal justice system has been one of the chief obstacles to improving the system.

In the past few years, however, there has been a substantial increase in the number, size and efficiency of criminal justice information systems throughout the country. Great emphasis has been placed on the development of systems for compiling and exchanging individual criminal histories or "rap sheets" because of the utility of this kind of information at all stages of the criminal justice process. Most of these systems are still manual, but some of the larger ones are automated at least in part and some of them are becoming quite sophisticated and efficient.

Of course, this increased efficiency has compounded security and privacy problems. In a real sense, the inefficiency of the old manual systems was the greatest protection of individual privacy. Files were scattered and access and dissemination was limited and slow. The computer has changed all that. The modern automated systems are characterized by rapid access and rapid dissemination. Although this might increase the potential damage of an inaccurate or incomplete criminal record, it is important to note that automated systems have provided security and privacy safeguards that were not possible in manual systems.

It is also important to keep in mind that these new systems dramatically increase the effectiveness of law enforcement. Computerized criminal justice information systems are essential to the effective administration of criminal justice and their use should be encouraged and facilitated as well as regulated by law. These systems can be operated in such a way as to meet all of the legitimate information needs of criminal justice agencies while providing adequate system security and protection against unreasonable invasions of personal privacy. Laws on security and privacy need not be so strict as to stifle the effectiveness of the systems. To deny to these systems the great benefits that derive from the technological advances in the field of information systems that have occurred in recent years would be a setback for the equitable administration of justice in our society.

Most of the criminal history systems in use today are for the most part manual systems and this will be true for many years to come. In fact, since the computerized NCIC–CCH system is in limited operation in only a few states, the only existing national system for exchanging criminal histories is the manual fingerprint identification system operated by the F.B.I. Care should be taken that a law designed primarily to deal with security and privacy problems growing out of national computerized systems not impose restrictions and requirements with which manual systems cannot possibly comply. Such a law should not contain provisions of general application that would unduly restrict many other forms of day-to-day operational recordkeeping, such as police blotters, court records and corrections records that do not present serious privacy risks.

ACCESS & USE

The State of Louisiana recommends that criminal offender record information be available for non-criminal justice purposes if "explicitly authorized" by state

or federal statute. We would not limit available records to conviction records, but we recommend that no information would be available concerning any individual who has not been convicted of at least one serious offense and has no such offense actively pending against him. A serious offense is one punishable by more than six months' imprisonment. This would help to preclude an individual's being unduly prejudiced by minor offenses. We believe this is a reasonable approach to a very difficult and controversial problem. In effect, it should be left to the States to authorize non-criminal justice uses of criminal records by explicit legislative enactments.

ARREST RECORDS

Probably the most controversial subjects is the matter of maintenance and dissemination of arrest records where no conviction results from the arrest. We believe that there are valid criminal justice uses for such arrest records and we urge careful consideration of legislation that would not permit such uses within limitations.

There are recorded instances where police officers have been killed or injured after stopping individuals who might have been approached more cautiously if the officer had been aware that the individuals had arrest records indicating that they were dangerous even though they had never been convicted. Arrest records also provide investigative leads in identifying suspects where there is no other information source available for the investigator to utilize.

REVIEW BY THE INDIVIDUAL

We recommend legislation that will permit the individual to inspect his criminal history record for the purpose of challenge or correction and provide for correction in appropriate cases. This is an extremely important safeguard against inaccurate and incomplete records. We also recommend that an individual who has obtained a copy of his record may not be required or requested to show or give it to anyone else. This is necessary to keep prospective employers or others from requiring individuals to obtain for them copies of criminal history records to which they are not entitled.

Another requirement we believe is important is a provision that any criminal record disseminated after its accuracy or completeness has been challenged shall include a notation informing the recipient of the challenge, also that any corrective action taken as a result of a challenge shall be communicated as soon as practicable (which means "immediately" in automated systems) to every criminal justice information system or agency that has received the erroneous information.

INTELLIGENCE SYSTEMS

Proposed federal legislation provides that criminal intelligence information shall not be maintained in criminal information systems that contain criminal histories, arrest records or other information on individual resulting from arrest, detention or adjudication. We agree with this separation requirement although we think it should be made clear that this does not preclude the maintenance in intelligence files of non-systematic references to arrests and convictions, so long as the two systems are kept separate and are not linked together in any way that would permit access to one system through the other.

The Louisiana Position on the issue of automated intelligence systems is:

(a) Criminal intelligence information regarding an individual may be entered into a criminal justice information system only if grounds exists connecting such individual with known or suspected criminal activity. Such systems shall review individual criminal intelligence files at least every two years to determine whether such grounds continue to exist, and shall immediately destroy all copies of criminal intelligence information relating to any individual as to whom such grounds do not exist.

(b) Access to and use of criminal intelligence information, including access by means of terminals or other equipment in the case of automated systems, shall be limited to law enforcement agencies, and, within such agencies, to components and individual officers or employees thereof determined by the agencies to have a need and a right to criminal intelligence information.

(c) No automated interstate criminal intelligence information system shall provide for dissemination of full criminal intelligence information records by means of remote computer terminal access to computerized data bases containing

such full records. Intelligence information disseminated by such means shall be limited to data sufficient to provide a register of index of the identities of individuals included in the systems and the names and locations of law enforcement agencies possessing criminal intelligence files relating to such individuals.

There is very strong consensus among Louisiana Law Enforcement agencies that intelligence systems are vital to law enforcement and should not be denied the benefits deriving from technological advances. Automated systems should be permitted, even on an interstate basis, because of the usefulness of such systems in investigating organized crime and other forms of criminal activity that crosses state lines. The controls imposed on intelligence systems should be strict, particularly in limiting dissemination to criminal justice officials as we have proposed. Such protections are necessary both for the subject and for the data in the system.

ACCURACY AND COMPLETENESS

As we have pointed out before, one of the most important factors in the protection of the rights of individuals about whom criminal records are maintained is the accuracy and completeness of the records. This is, of course, also an important factor in the usefulness of the records to criminal justice agencies.

PRECEDENCE OF STATE LAWS

A comment of one other aspect we consider to be very important—the relationship between state and federal laws.

Like most State officials, we are extremely sensitive about federal laws that overrule state laws, or federal laws that condition federal funding of state and local activities. In our opinion neither the interstate nature of some of these information systems nor the federal funding that has gone into them justifies the enactment of a federal law and the promulgation of federal regulations that will in effect nullify adequate state laws on the subject of security and privacy. I also ask that consideration be given to the possible impact of the administrative and procedural problems imposed by federal laws. We urge that a limit be placed on the application of any bill you impose on those states that do not now have adequate laws to protect the privacy of individuals and do not enact such laws within a reasonable period. Perhaps if the effective date of the federal law were delayed for at least two years that would spur most states to act. After that time the federal law would be effective in those states that have not enacted their own laws.

STATE OF LOUISIANA,
DEPARTMENT OF JUSTICE,
Baton Rouge, July 1, 1974.

To: All Law Enforcement, Prosecutors, Courts, Probation/Parole and Correctional Agencies Having Access to and Responsibility for the Security of Criminal Offender Record Information.

Concerned about the potential misuse of criminal justice data on individuals made possible by rapid automation of criminal data systems and accelerating computer technology, Congress added an amendment to the Omnibus Crime Control and Safe Streets Act of 1970 directing the U.S. Department of Justice to draft legislation for consideration by the Congress to insure the security and confidentiality of individualized criminal data. As a result, two highly significant bills, (S. 2963) by Senator Ervin (N.C.) and (S. 2964) by Senator Hruska (Neb.), have been introduced defining the parameters of security and confidentiality in criminal justice information systems. In a separate but related action, the Law Enforcement Assistance Administration (LEAA) published its guidelines on the same subject in the February 14, 1974 *Federal Register*. These guidelines will determine standards for federal, state and local criminal data systems until and unless superseded by federal legislation.

Computerized criminal justice information systems are essential to the effective administration of criminal justice and their use should be encouraged and facilitated as well as regulated by law. These systems can be operated in such a way as to meet all the legitimate information needs of criminal justice agencies while providing adequate system security and protection against unreasable invasions of personal privacy.

Section 577 of Part 1 of Chapter 6 of Title 15 of the Louisiana Revised Statutes of 1950, as amended requires that the Department of Justice (Office of the Attorney General) "adopt such measures to assure the security of the system as may be specified in state and federal regulations".

With this in mind, I have caused to be issued the attached Privacy and Security Regulations which are designed to insure the protection of an individuals computerized criminal offender record from improper or illegal use.

Respectfully submitted,

WILLIAM J. GUSTE, JR., *Attorney General.*

LCJIS PRIVACY/SECURITY REGULATIONS

The enclosed regulations were designed to serve the purpose of protecting the automated record of an individual criminal offender from improper and/or illegal use. Beginning with a definition of the contents of the offender's criminal record, these regulations also clearly define and delegate authority for access to this information. Procedures are provided to change the record in the event of inaccurate content, and allow unauthorized persons or agencies who wish to access the record for legitimate reasons to obtain access. Security measures that must be taken to protect the record, including computer programming and personnel security as well as training requirements for systems personnel are fully described. Finally, a regulation is set forth herein which defines a function of the Attorney General's office to inform and educate the general public about the Privacy and Security Regulations.

All Louisiana criminal justice agencies are expected to conform with these regulations and any amendment to such. Please be advised that all agencies in the enclosed mailing list with asterisks beside their name will be furnished an information copy only and will not receive updates or amendments. All other agencies will receive one copy of the regulations and any forthcoming amendments. Agencies are authorized to reproduce these regulations for any additional copy needs.

LOUISIANA DEPARTMENT OF JUSTICE.
Baton Rouge, La., July 1, 1974.

LCJIS REGULATION NO. 1-01

TABLE OF CONTENTS AND SUBJECT INDEX

Purpose: This regulation sets forth an index to all LCJIS Regulations Series 1 by both numerical order and subject matter.

1. Table of Contents

No. Title

1-01 Table of Contents and Subject Index
Purpose: This regulation sets forth an index to all LCJIS Regulations Series 1 by both numerical order and subject matter.

1-02 Administrative Procedures
Purpose: This regulation sets forth the requirements and procedures for the issuance of new and/or revised regulations.

1-03 General Regulation
Purpose: This is a general regulation limiting the applicability of all LCJIS Regulations Series 1 to the State of Louisiana and to the rules of evidence and procedure of that state.

1-04 Definitions
Purpose: This regulation defines the technical terms for all LCJIS Regulations Series 1.

1-05 The Content of Criminal Offender Record Information
Purpose: This regulation defines the content of the criminal offender record information and the procedure by which the record can be challenged for accuracy or completeness.

1-06 Eligibility for Access to Computerized Criminal Offender Record Information
Purpose: This regulation defines who has access to computerized criminal offender record information and the procedures taken to protect these records from illegal use. This regulation allows criminal justice agencies, authorized researchers, and individuals in the system the right to have access to the record(s).

In order to protect these records from illegal use, persons having access to the records must sign a non-disclosure agreement. Action taken for violation of this privileged information is defined in the administrative penalties.

Appendix A: LCJIS Form No. 1: Review of Criminal Offender Record Information.

Appendix B: LCJIS Form No. 2: Exceptions Taken to Criminal Offender Record Information.

Appendix C: LCJIS Form No. 3: Notice of Results of Audit of Criminal Offender Record Information.

1-07 Listing of Agencies to Which Criminal Offender Record Information has been Disseminated

Purpose: This regulation defines the procedure for listing of agencies to which criminal offender record information has been disseminated.

1-08 Segregation of Computerized Files and their Linkage to Intelligence Files

Purpose: This regulation defines the type of computer recommended for use in the storage of criminal offender record information and the linkage of these records to intelligence files.

1-09 Programming Security

Purpose: This regulation defines the procedures for programming security in order to assure the continued security of criminal offender record information under their control. These procedures will include, but not be limited to the following: terminal and operator identification, data storage, data entry, and file protection software.

1-10 Physical Security

Purpose: This regulation defines physical security in terms of protection from accidental loss and intentional damage to the system.

1-11 Personnel Security

Purpose: This regulation defines the procedure by which personnel security is achieved and maintained. The procedure includes employment screening, clearance, annual review/security manual and in-service training, and system discipline.

1-12 Training of System Personnel

Purpose: This regulation defines the length of time and the type of training all persons involved in the direct operation of a criminal offender record information system shall receive.

1-13 Public Education

Purpose: This regulation defines a function of the Attorney General which is to conduct an appropriate program of public education concerning the purposes, proper use and control of criminal offender record information.

2. *Subject Index*

1-02 Administrative Procedures
1-05 The Content of all Offender Record Information
1-04 Definitions
1-06 Eligibility for Access to Computerized Criminal Offender Record Information

Appendix A: LCJIS Form No. 1: Review of Criminal Offender Record Information

Appendix B: LCJIS Form No. 2: Exceptions Taken to Criminal Offender Record Information

Appendix C: LCJIS Form No. 3: Notice of Results of Audit of Criminal Offender Record Information

1-03 General Regulation
1-07 Listing of Agencies to Which Criminal Offender Record Information has been Disseminated
1-11 Personnel Security
1-10 Physical Security
1-09 Programming Security
1-13 Public Education
1-08 Segregation of Computerized Files and Their Linkage to Intelligence Files
1-10 Table of Contents and Subject Index
1-12 Training of System Personnel

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Honorable WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS Regulation No. 1–02

ADMINISTRATIVE PROCEDURES

Purpose: This regulation sets forth the requirements and procedures for the issuance of new and/or revised regulations.

Authority

Revision notices, changes and/or issuance of new regulations must have the final approval of the LCJIS Policy Board and the Attorney General.

Procedures for Changes

1. Recommended changes to these regulations shall be directed to the Chairman, LCJIS Privacy/Security Committee, Room 502, 1885 Wooddale Blvd., Baton Rouge, La. 70806.
2. All recommended changes will be presented to the Privacy/Security Committee for review. They will then forward their recommendations along with the request to the LCJIS Policy Board for review and approval/disapproval action. Upon approval, the document will be sent to the Attorney General for final approval, publication and distribution.
3. All disapproved requests will be returned to the originator with appropriate comments as to the reason(s) for disapproval.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Honorable William J. Guste, Jr.,
Attorney General.

LCJIS Regulation No. 1–03

GENERAL REGULATION

Purpose: This is a general regulation limiting the applicability of all LCJIS Regulations Series 1 to the State of Louisiana and to the rules of evidence and procedure of that state.

1. *Limitation to this State*—Except as otherwise provided in these regulations or in any applicable statutory provision, these regulations shall be applicable only within this state, and all references to criminal justice agencies shall, unless otherwise provided, be understood to mean such agencies organized and operating under the laws of this state.
2. *Rules of Evidence and Procedure*—Except as otherwise provided in these regulations or in any applicable statutory provisions, or except as the Department may otherwise decide, the rules of evidence and procedure applicable to any hearings or inquiries conducted by the Department or LCJIS Privacy/Security Committee shall be those in use for civil proceedings in the courts of this state at the time of the hearing or inquiry.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Honorable William J. Guste, Jr.,
Attorney General.

LCJIS Regulation No. 1–04

DEFINITIONS

Purpose: This regulation defines the technical terms for all LCJIS Regulations Series 1.

Definitions for purposes of these regulations:

1. The term "criminal justice agencies" means only those public agencies at all levels of government which perform as their principal function activities (i) relating to the apprehension, prosecution, adjudication, or rehabilitation of criminal offenders; or (ii) relating to the collection, storage, dissemination or usage of criminal offender record information. This definition includes, at the local or regional level, municipal law enforcement agencies, sheriffs, district or city courts having a criminal jurisdiction, district attorneys, city prosecutors, probation departments and parish and multi-parish prisons. State agencies in

this category are the Division of State Police of the Department of Public Safety, Department of Corrections, Supreme Court and Department of Justice.

2. The term "criminal offender record information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, rehabilitation and release. Such information shall be understood to be restricted to that recorded as the result of the initiation of criminal proceedings or of any consequent proceedings related thereto. It shall be understood not to include intelligence, analytical and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

3. The "Committee" and "Department" shall respectively be understood to mean the Security and Privacy Committee and the Louisiana Department of Justice.

4. The term "judge" shall be understood to encompass both "close" and "expunge".

5. The term "close" shall be understood to mean the retention of files, records or information subject to such restrictions upon access to and dissemination of such files, records or information as are required by these regulations.

6. The term "expunge" shall be understood to mean the physical destruction of files, records or information.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION NO. 1-03

THE CONTENT OF CRIMINAL OFFENDER RECORD INFORMATION

Purpose: This regulation defines the content of the criminal offender record information and the procedure by which the record can be challenged for accuracy or completeness.

1. The Content of Criminal Offender Record Information

Criminal offender record information shall be understood to be confined to that generally contained in "rap sheets". That is to say, such information shall be confined to a recording of personal identifying facts and of the results of an arrested individual's movement through the various formal stages of the criminal justice process, from arrest through trial, if any, disposition and release. Intelligence data and informal or subjective comments regarding an individual's behavior or attitudes shall not be understood to be criminal offender record information. The following rules apply to computerized criminal offender record information:

(*a*) Individual record information entered in a person's file shall be relevant to the purpose for which the file was created.

(*b*) Misdemeanor, drunk and traffic records where the case did not result in imprisonment or probation supervision shall not be entered in computerized criminal offender files.

(*c*) Misdemeanor arrests not leading to conviction shall be subject to expungement in accordance with existing law.

(*d*) Information that arrest took place or prosecution was initiated shall not be entered in a computerized criminal offender file without subsequent entry of a final law enforcement or judicial disposition.

(*e*) Individual record information which is anecdotal, evaluative, or judgmental shall not be computerized; provided that where an agency's responsibilities require behavioral analysis of individuals, that agency may automate standardized personal evaluation data entries of a type useful for research classification.

(*f*) Each criminal justice agency maintaining records in an "in-process" criminal offender file must ensure that the most current record is used or obtained. Entries which are not current or accurate should be eliminated from the system.

2. Challenges to the Accuracy or Completeness of Automated Criminal Offender Record Information

(*a*) Any person who believes that automated criminal offender record information which refers to him is inaccurate, incomplete, or misleading may request the originating criminal justice agency in this state to purge, modify, or supplement that information. See section2 3(f) of Regulation 1–06. Should the agency decline so to act, or should the individual believe the agency's decision to be otherwise unsatisfactory, the individual may request review by the Committee.

(*b*) Such requests to the Committee shall be made in writing. Each request shall include a concise statement of the alleged deficiencies of the criminal offender record information, shall state the date and result of any review by the criminal justice agency, and shall append a sworn vertification of the facts alleged in the request signed by the individual or his attorney.

(*c*) Upon receipt of each such request, the Committee shall ask any criminal justice agency which has previously reviewed the criminal offender record information to provide the Committee a written summary of the review and of its findings.

(*d*) A hearing officer, selected by the Committee from among its members or staff, shall, upon the basis of the request and/or the summary and any other statements or documents provided by the individual or by the criminal justice agency, determine whether there is prima facie evidence that the criminal offender record information is inaccurate, misleading, or incomplete. Should the hearing officer find that there is no such evidence, the individual may seek review by the Committee. See subsection (g). Should the hearing officer find that there is such evidence, the Committee shall empanel a review tribunal from among its members and staff. The tribunal shall consist of not less than three members, a majority of which shall be members of the Committee. The individual and each criminal justice agency with custody or control of the information in question may challenge for cause any members of the tribunal or hearing officer. Each such challenge shall be decided by majority vote of the full Committee.

(e) The tribunal may require the individual or any criminal justice agency withi nthe state to file written statements, arguments or documenary materials. It may impose such time requirements for these purposes as it deems appropriate. Unless the individual walves in writing his right to a hearing, the tribunal shall conduct a public hearing at which the individual may appear with counsel, may present evidence, and may examine and cross-examine witnesses. The rules of evidence and procedure in use by the courts of this state for civil proceedings at the time of the hearing shall, except insofar as the Committee may otherwise decide, be applied by the tribunal.

(*f*) The tribunal shall issue written findings and conclusions, in which any relief to which it believes the individual is entitled shall be fully and specifically described. The tribunal may with respect to cases which it believes to be either unusually difficult or of general importance, certify the request to the full Committee for review. Findings and conclusions, as well as such certifications, shall be adopted by majority vote of the tribunal.

(*g*) Should the individual or any criminal justice agency with custody or control of the information in question believe the findings or conclusions of a hearing officer or tribunal to be unsatisfactory, the individual or agency may petition the full Committee for review. Each such petition, and each certification from a tribunal under the terms of subsection (f), shall be voted upon by the Committee, and review shall be granted whenever three or more members of the Committee vote that it should be granted. The Committee may, when it grants review, permit oral argument and the presentation of other evidence. Where review is granted of the findings of a hearing officer, the Committee may empanel a review tribunal and submit the request for decisions by that tribunal. Where the Committee conducts a review, it shall issue written findings and conclusions.

(*h*) The final disposition of each request, whether upon the basis of the findings and conclusions of a hearing officer, a tribunal, or the Committee shall be by order of the Committee.

(*i*) Where the final disposition of a request includes an order that criminal offender record information be purged, modified, or supplemented, that order

shall be promptly communicated by the Committee to the Department. The Department shall in each such case promptly transmit the terms of the order to all criminal justice agencies within the state, to the individual involved, and to all other individuals or agencies, whether or not located within this state, to which the criminal offender record information in question has previously been communicated. The individuals and agencies to which such information has previously been communicated shall be determined by examination of the listings required to be maintained by Regulation 1–07.

(*j*) Records challenged under the provisions of these regulations shall be deemed to be accurate, complete and valid until otherwise ordered by the Committee.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, JR.,
Attorney General.

LCJIS REGULATION No. 1–06

ELIGIBILITY FOR ACCESS TO COMPUTERIZED CRIMINAL OFFENDER RECORD INFORMATION

Purpose: This regulation defines who has access to computerized criminal offender record information and the procedures taken to protect these records from illegal use. This regulation allows criminal justice agencies, authorized researchers, and individuals in the system the right to have access to the record(s). In order to protect these records from illegal use, persons having access to the records must sign a non-disclosure agreement. Action taken for violation of this privileged information is defined in the administrative penalties.

1. Criminal Justice Agencies

Criminal justice agencies shall be permitted to have access to computerized criminal justice information systems where they have both a need and a right to know. Non-criminal justice information shall be supplied with such information only through criminal justice agencies.

Criminal offender record information may be disseminated to federal agencies and the agencies of other states and jurisdictions only if they are criminal justice agencies within the meaning of these regulations.

Unless certified as a qualified criminal justice agency by the Department, each agency in this state that wishes access to criminal offender record information shall in writing request the Department to make a finding of its eligibility for such access. The Department shall promptly make and issue written findings as to each such agency's eligibility or non-eligibility for such access. Upon request by the agency or any other interested party, or upon the Department's own motion, the Department may conduct public hearings at which it may receive evidence and hear statements and arguments from any interested parties.

2. Research Use of Criminal Offender Record Information

(*a*) Research Design and Access to Information. Researchers who wish to use criminal justice information shall first submit to the Security and Privacy Committee a completed research design that guarantees adequate protection of security and privacy. Authorization to use criminal justice information shall only be given when the Committee has approved the research design.

The Committee shall recommend to a criminal justice agency that a particular research program should be permitted access to criminal offender record information only if it finds that any threats to individual privacy created by the program:

(1) Have been minimized by methods and procedures reasonably calculated to prevent injury or embarrassment to individuals and;

(2) are clearly outweighed by the advantages for the criminal justice system that may reasonably be expected to result if the program is permitted.

The decision of the Committee to permit or not to permit any program of research shall not be binding upon any other criminal justice agency.

(*b*) Limits on Criminal Justice Research. Research shall preserve the anonymity of all subjects.

The following requirements shall be applicable to all such programs of research, and each criminal justice agency and researcher shall be responsible for their full and prompt implementation.

(1) In no case shall criminal offender record information furnished for purposes of any program of research be used to the detriment of the persons to whom such information relates.

(2) In no case shall criminal offender record information furnished for purposes of any program of research be used for any other purpose; nor shall such information be used for any program of research other than that authorized and approved by the Committee.

(3) Each participant and employee of every program of research authorized access to criminal offender record information shall, prior to having such access, fully and completely execute a non-disclosure agreement approved by the Committee.

(4) In every case the authorization for access to criminal offender record information shall assure the criminal justice agency and the Committee full and complete rights to monitor the program of research to assure compliance with this regulation. Such monitoring rights shall include the right of the Committee to audit and review such monitoring activities and also to pursue its own monitoring activities.

(5) Each such program of research shall preserve the right of the Committee and the criminal justice agency involved to examine and verify the data generated as the result of the program, and, if a material error or omission is found to have occurred, to order that the data not be released for any purpose unless corrected to the satisfaction of the agency or Committee.

(c) Duties and Responsibilities of the Holding Agency. Each criminal justice agency shall formulate methods and procedures to assure compliance with the requirements of this regulation with respect to the use of criminal offender record information for purposes of any program of behavioral or other research, whether such programs are conducted by a criminal justice agency or by any other agency or person. Each criminal justice agency releasing crirminal offender information for research purposes shall maintain a listing of the agencies or individuals to which such information is released. Such listings shall be subject to the requirements prescribed in Regulation 1-07. The Committee may require any modifications or additions to these methods and procedures that it finds necessary for full and prompt compliance with this regulation.

3. *Individual's Right to Review Automated Criminal Offender Record Information*

Each individual shall have the right to review automated criminal offender record information relating to him. Each criminal justice agency in this state with custody or control of criminal offender record information shall make available facilities and personnel necessary to permit such reviews. Such reviews shall be conducted in accordance with the following procedures:

(a) Such reviews shall occur only within the facilities of a criminal justice agency and only under the supervision and in the presence of a designated employee or agent of a criminal justice agency. The files and records made available to the individual shall not be removed from the premises of the criminal justice agency.

(b) Such reviews may, at the discretion of each criminal justice agency, be limited to ordinary daylight business hours.

(c) Such reviews shall be permitted only after proper verification that the requesting individual is the subject of the criminal offender record information which he seeks to review. Each criminal justice agency shall require fingerprinting for this purpose. Upon presentation of a sworn authorization from the individual involved, together with proof of identity, an individual's attorney may be permitted to examine the criminal offender record information relating to the individual.

(d) A record of each such review shall be maintained by each criminal justice agency by the completion and preservation of LCJIS Form No. 1. (See Appendix A) Each such form shall be completed and signed by the supervisory employee or agent present at the review. The reviewing individual shall be asked, but may not be required, to verify by his signature the criminal offender record information he has reviewed. The form shall include a recording of the name of the reviewing individual, the date of the review, and whether or not any exception was taken to the accuracy, completeness or contents of the information reviewed.

(e) The reviewing individual may make a written summary or notes in his own handwriting of the information reviewed, and may take him such copies. Such individuals may not, however, take any such copy that might reasonably

be confused with the original. Criminal justice agencies are not required to provide equipment for copying.

(*f*) Each individual shall be informed of his rights of challenge under this regulation. Each such individual shall be informed that he may submit written exceptions as to the information's contents, completeness or accuracy to the criminal justice agency with custody or control of the information. Should the individual elect to submit such exceptions, he shall be furnished LCJIS Form No. 2 (See Appendix B). The individual shall record any such exceptions on the form. The form shall include an affirmance, signed by the individual or his legal representative, that the exceptions are made in good faith and to the best of the individual's knowledge are believed true. One copy of the form shall be forwarded to the review officer of the criminal justice agency in question. An officer shall be designated for that purpose in each criminal justice agency. A second copy of the form shall be forwarded to the Department. The criminal justice agency shall in each case cause to be conducted an audit of the individual's criminal offender record information appropriate to determine the accuracy of the exceptions. The Department and the individual shall be informed in writing of the results of the audit. LCJIS Form No. 3 (See Appendix C) may be used for this purpose. Should the audit disclose inaccuracies or omissions in the information, the criminal justice agency shall cause appropriate alterations or additions to be made to the information and shall cause notice of such alterations or additions to be given to the Department, the individual involved, and any other agencies in this or any other jurisdiction to which that criminal offender record information has previously been disseminated.

4. No Other Access to Criminal Offender Record Information Shall be Permitted Except as Required by Valid State Statutes

5. Non-disclosure Agreement

No agency qualified under these regulations to obtain computerized criminal justice information may obtain access until it has signed a non-disclosure agreement, as adopted by the Security and Privacy Committee.

6. Administrative Penalties:

(*a*) Any violation of the provisions of these regulations committed by any employee or officer of any public agency of this state, in addition to any applicable criminal or civil penalties, shall be punished by suspension, discharge, reduction in grade, transfer or such other administrative penalties as are deemed by the criminal justice agency to be appropriate. Provided, however, that such penalties shall be imposed only if they are permissible under any applicable statutes governing the terms of employment of the employee or officer in question.

(*b*) Where any public agency of this state is found by the Department willfully or repeatedly to have violated the requirements of these regulations, the Department may where other statutory provisions permit, prohibit the dissemination of criminal offender record information to that agency, for such periods and on such conditions as the Department deems appropriate.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LSJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, JR.,
Attorney General.

LCJIS REGULATION NO. 1-06

APPENDIX A

LCJIS FORM NO. 1

Date _____

REVIEW OF CRIMINAL OFFENDER RECORD INFORMATION

1. Name and location of agency: _____
2. Name of supervisory employee: _____
3. Name of reviewing individual: _____
4. Record reviewed: _____
   Name of individual to whom records relate: _____
   Identification number: _____

5. Did the reviewing individual express any challenge to the accuracy or completeness of the information reviewed? ——— If he did so, to what portions the information?_____
6. Verification: *Note: Completion of this item is voluntary.*
I have reviewed the records described above and have found no errors or omissions therein.

_____
Signature of reviewing individual

Date of Verification: _____
7. Note: Each reviewing individual shall be informed of his rights of challenge under these regulations.

APPENDIX B

LCJIS FORM No. 2

EXCEPTIONS TAKEN TO CRIMINAL OFFENDER RECORD INFORMATION

1. Name of individual submitting exceptions: _____
_____
2. Name of agency: _____
3. Records to which exceptions taken: _____
_____
_____
Name of individual to whom records relate: _____
Identification number: _____
4. Summary of exceptions and reasons therefor: _____
_____
_____
_____
5. Verification.
I affirm that I have taken the above-described exceptions, that those exceptions are taken in good faith, and that they are to the best of my knowledge true.

_____
Signature of Individual

Date of verification: _____

APPENDIX C

LCJIS FORM No. 3

NOTICE OF RESULTS OF AUDIT OF CRIMINAL OFFENDER RECORD INFORMATION

To: _____
_____
_____

Pursuant to exceptions taken on _____, 19_____, by _____ to criminal offender record information within the custody or under the control of _____, an audit of the information has been conducted and, in accordance with the results of that audit, the exceptions have been _____
_____

The following actions have been taken, or now are in progress, to implement the audit's findings:

(Name of criminal justice agency conducting the audit.)

Dated: _____

LCJIS Regulation No. 1–07

LISTING OF AGENCIES TO WHICH CRIMINAL OFFENDER RECORD INFORMATION HAS BEEN DISSEMINATED

Purpose: This regulation defines the procedure for listing of agencies to which criminal offender record information has been disseminated.

Listing of Agencies to Which Criminal Offender Record Information Has Been Disseminated

Each criminal justice agency in this state shall maintain a listing of the agencies or individuals, both in and outside this state, to which it released criminal offender record information. Each such listing is to be preserved for a period of not less than one year from the date of the release to which it relates. Such listings may be maintained in whatever form criminal justice agencies may elect, but each such listing shall indicate the agency or individual to which information was released, the date of the release, the individual to whom the information relates, and the items of information released. Such listings shall be made available for audit or inspection by the Department, the Committee, or their staff members at such times as the Department or Committee may require.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. William J. Guste, Jr.,
Attorney General.

LCJIS Regulation No. 1–08

SEGREGATION OF COMPUTERIZED FILES AND THEIR LINKAGE TO INTELLIGENCE FILES

Purpose: This regulation defines the type of computer recommended for use in the storage of criminal offender record information and the linkage of these records to intelligence files.

1. Segregation of Computerized Files

All criminal offender record information should be stored in a computer dedicated solely to criminal justice users. However, where this is not immediately possible, efforts should continue towards the goal of a dedicated computer. Where existing limitations temporarily prevent the use of a solely dedicated computer, the data files and programs used by the criminal justice system shall be under the management control of a criminal justice agency and shall be dedicated in the following manner:

(*a*) Files shall be stored on the computer in such a manner that they cannot be modified, destroyed, accessed, changed, or overlaid in any fashion by non-criminal justice terminals.

(*b*) The agency employee in charge of computer operations shall write and install, or cause to have written and installed, a program that will prohibit inquiry, file updates or destruction from any terminal other than criminal justice system terminals which are so designated. The destruction of files shall be limited to specifically designated terminals under the management control of the criminal justice agency responsible for maintaining the files.

(c) The agency employee in charge of computer operations shall write and install, or cause to have written and installed, a classified program to detect and store for classified output all attempts to penetrate any criminal offender record information system, program or file. This program shall be known only to the agency control employee and his immediate assistant and the records of such program shall be kept continuously under maximum security conditions. No other persons, including staff and repair personnel, shall be permitted to know this program.

(d) Non-terminal access to criminal offender record information such as requests for tapes, file dumps, printouts, etc., shall be permitted only with approval of the criminal justice agency having management control of the data. The employee in charge of computer operations shall forward all such requests to the criminal justice agency employee responsible for maintaining systems and data security.

2. Linkage to Intelligence Files

(a) Criminal offender record files may be linked to intelligence files in such a manner that an intelligence inquiry from a criminal justice terminal can trigger a printout of the subject's criminal offender record information.

(b) A criminal offender record inquiry response shall not include information which indicates that an intelligence file exists.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION NO. 1–09

PROGRAMMING SECURITY

Purpose: This regulation defines the procedures for programming security in order to assure the continued security of criminal offender record information under their control. These procedures will include, but not be limited to the following: terminal and operator identification, data storage, data entry, and file protection software.

1. Terminal and Operator Identification:

(a) There shall be a terminal identification code number for each remote terminal as a precondition for entering the files (normally done by software).

(b) Within each agency, terminal use shall be assigned to a limited and identified group of individuals.

(c) Each individual terminal user shall identify himself by a personal identification number or authorization code.

(d) The computer shall be programmed to log the identity of all users, the files accessed, and the date of access. This information shall be maintained for twelve (12) months.

(e) Each remote terminal user shall establish a written log of terminal use, which shall be audited periodically.

2. Data Storage

(a) Where a computer file may be accessed by more than one agency, system software shall ensure that each agency shall obtain only the data to which it is entitled.

(b) System hardware and software shall contain controls to ensure that each user with on-line direct terminal access can obtain only reports authorized for its use.

(c) System software shall be implemented to erase and clear core, buffers, mass storage, and peripheral equipment of data automatically whenever purging is required by these regulations.

(d) Duplicate computer files shall be created as a counter-measure for destruction of original files and all computer tapes or discs shall be locked in a safe storage area under the control of senior personnel. Secondary storage should be used for back-up.

3. Data Entry:

(a) Where criminal justice data is transmitted to a data center on reporting forms, the center shall establish procedures for destroying these forms after the data is entered in the computer.

(*b*) System software shall contain controls to ensure that each terminal is limited to the information it can input, modify, or cancel.

4. File Protection Software:

(*a*) A monitor program shall be developed to report attempts to violate the system security software.

(*b*) Edit programs shall be created to periodically audit record alteration transactions.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION No. 1–10

PHYSICAL SECURITY

Purpose: This regulation defines physical security in terms of protection from accidental loss and intentional damage to the system.

1. Protection from Accidental Loss

Information system managers shall institute procedures for protection of information from environmental hazards including fire, flood, and power failure. Appropriate elements should include adequate fire detection and quenching systems, watertight facilities, protection against water and smoke damage, liaison with local fire and public safety officials, fire resistant materials on walls and floors, air conditioning systems, emergency power sources, and backup files.

2. Intentional Damage to System

Agencies administering criminal justice information systems shall adopt security procedures which limit access to information files. These procedures should include use of guards, keys, badges, passwords, access restrictions, sign-in logs, or like controls. All facilities which house criminal justice information files shall be so designed and constructed as to reduce the possibiilty of physical damage to the information. Appropriate steps in this regard include: pyhsical limitations on access, security storage for information media, heavy duty non-exposed walls, perimeter barriers, adequate lighting, detection and warning devices and closed circuit television.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION No. 1–11

PERSONNEL SECURITY

Purpose: This regulation defines the procedure by which personnel security is achieved and maintained. The procedure includes employment screening, clearance, annual review/security manual and in-service training, and system discipline.

1. Employment Screening

Applicants for employment and those presently employed in criminal justice information systems shall be expected to consent to an investigation of their character, habits, previous employment, and other matters necessary to establish their good moral character, reputation, and honesty. Giving false information should disqualify an applicant from employment and subject a present employee to dismissal.

Investigation should be designed to develop sufficient information to enable the appropriate officials to determine employability and fitness of persons entering sensitive positions. Investigations of applicants should be conducted on a pre-employment basis and the resulting reports used as a personnel selection device.

2. Clearance, Annual Review/Security Manual and In-Service Training

System personnel including terminal operators in remote locations, as well as programmers, computer operators, and others working at or near the central processor, shall be assigned appropriate security clearances and should have those clearances renewed periodically after investigation and review.

Each criminal justice information system shall prepare a security manual listing the rules and regulations applicable to maintenance of system security. Each person working with or having access to criminal justice information files should know the contents of the manual. To this end, each employee should receive not less than four (4) hours of training each year concerning system security.

3. System Discipline

The management of each criminal justice information system should establish sanctions for accidental or intentional violation of system security standards. Supervisory personnel should be delegated adequate authority and responsibility to enforce the system's security standards.

Any violation of the provisions of these standards by any employee or officer of any public agency, in addition to any applicable criminal or civil penalties, shall be punished by suspension, discharge, reduction in grade, transfer or such other administrative penalties as are deemed by the criminal justice agency to be appropriate; provided, however, that such penalties shall be imposed only if they are permissible under any applicable statutes governing the terms of employment of the employee or officer in question.

Where any public agency is found by the Committee willfully or repeatedly to have violated the requirements of the standard, the Committee may, where other statutory provisions permit, prohibit the dissemination of criminal offender record information to that agency, for such periods and on such conditions as the Committee deems appropriate.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION No. 1-12

TRAINING OF SYSTEM PERSONNEL

Purpose: This regulation defines the length of time and the type of training all persons involved in the direct operation of a criminal offender record information system shall receive.

Training of System Personnel

All persons involved in the direct operation of a criminal offender record information system shall receive a total of not less than four (4) hours, and all immediate supervisors of such persons shall receive a total of not less than six (6) hours of approved instruction concerning the proper use and control of criminal offender record information and related systems. Instruction may be offered by any agency or facility, provided that the course of instruction, materials, and qualifications of instructors have been reviewed and approved by the Department. Each such operator or supervisor shall begin to attend such a course of instruction within a reasonable period of time after assignment to the criminal offender record information system.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

LCJIS REGULATION No. 1-13

PUBLIC EDUCATION

Purpose: This regulation defines a function of the Attorney General which is to conduct an appropriate program of public education concerning the purposes, proper use and control of criminal offender record information.

Public Education

The Attorney General shall conduct an appropriate program of public education concerning the purposes, proper use and control of criminal offender record information. He may make available upon request facilities, materials, and personnel for the purpose of educating the public about the purposes, proper use and control of criminal offender record information.

This regulation has been reviewed and approved by the LCJIS Privacy and Security Committee and the LCJIS Policy Board.

Approved:

Hon. WILLIAM J. GUSTE, Jr.,
Attorney General.

STATE OF MAINE

OFFICE OF THE GOVERNOR,
Augusta, Maine, July 2, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, U.S. Senate Committee
on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: Thank you for sending me copies of your co-sponsored legislation concerning information systems and individual privacy.

I certainly endorse such legislation in concept and I appreciate the opportunity to review the details of your proposals.

Sincerely,

KENNETH M. CURTIS, *Governor.*

STATE OF NEBRASKA

DEPARTMENT OF JUSTICE,
Lincoln, Nebr., July 8, 1974.

Hon. SAM J. ERVIN, Jr.,
U.S. Senator,
Senate Office Building,
Washington, D.C.

DEAR SENATOR: In your June 25 letter you ask for comment on the desirability and practicability of the provisions contained in S. 3418, which would deal with personal information systems.

In Sec. 202(2) of the proposal an exemption is created for personal information systems "which are part of active criminal investigatory files compiled by Federal, State, or local law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution * * *." I would urge that this exemption be re-worded to exclude from the act all criminal justice information which is covered by your other bill dealing with the security and privacy of criminal justice information. There are going to be enough problems in getting the criminal justice bill into operation, without compounding them by mixing the two bills.

I am forwarding a copy of your letter, and its enclosures, to the department of Nebraska state government which is actively engaged in studying our computer and data bank needs, with the thought that they are better qualified to comment on other parts of your proposal.

Sincerely,

CLARENCE A. H. MEYER,
Attorney General.

STATE OF NEVADA

OFFICE OF THE ATTORNEY GENERAL,
Carson City, September 18, 1974.

Hon. SAM J. ERVIN, JR.,
Chairman, Committee on Government Operations, U.S. Senate,
Washington, D.C.

DEAR SENATOR ERVIN: In your letter of June 25, 1974, you requested this office to review and comment upon the provisions of S. 3418, a bill to establish standards and safeguards on the collection, maintenance and dissemination of information on individuals by public and private information systems.

We have now completed our review of the bill and find ourselves generally in accord with its objectives.

The rapid expansion of information systems in the last two decades through increased use of computers poses a serious challenge to the rights of all Americans to live in an atmosphere of relative privacy. Of course, modern life would not be

possible without some collection, maintenance and dissemination of personal information about individuals, but it is important that institutions which engage in such activities, be they public or private, do so only to the extent absolutely necessary to the accomplishment of their legitimate purposes. Every effort should be made to eliminate questions or other information concerning individuals which are irrelevant.

The opportunity provided by S. 3418 for an individual to challenge, correct or explain information about him in an information system not only is an essential right of every citizen, but is equally important to the agency which maintains the information since accuracy of information contained in the system is basic to any decision to be made with respect to that particular individual.

Quite frankly, we do envision some difficulty in complying with that provision of your bill which requires prior permission of a "data subject" to disseminate information to another organization or system not having regular access authority. Our concern arises partly from the fact that the bill contains no definition of the phrase "organization or system having regular access authority" and partly because keeping any up to date mailing addresses on all persons for whom a file or other information is maintained is a task of herculean proportions.

We also have some reservation about that provision of S. 3418 which limits dissemination of information by federal agencies only to authorized employees of other federal agencies. Particularly in the area of licensing professions and other occupations, exchanges of information between government agencies at the federal, state and local levels may be critical to a proper evaluation of professional credentials. Some broadening of this language may be appropriate.

One final observation which we would like to make involves a possible conflict between the provisions of S. 3418 and the policy considerations behind a public records law like Nevada Revised Statutes, Chapter 239. Our state enactment is intended to provide maximum public access to the files of state and local government. Your bill has a quite different purpose. Should S. 3418 become law, it likely will have a serious impact upon state laws relating to public records in Nevada and other states, especially in view of the fact that courts are constantly broadening the definition of the term "public records" to include information and files which only a few years ago we all considered private and confidential.

We appreciate this opportunity to express our views on your proposed legislation. If we may be of any further assistance on this matter or other matters of mutual concern, please advise.

Sincerely,

ROBERT LIST, *Attorney General.*
By JAMES H. THOMPSON, *Chief Deputy Attorney General.*

STATE OF NEW MEXICO

OFFICE OF THE ATTORNEY GENERAL,
DEPARTMENT OF JUSTICE,
Santa Fe, N. Mex., July 8, 1974.

Senator SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
Senate Office Building, Washington, D.C.

DEAR SIR: This is in reply to your letter of June 25, 1974 requesting information on the right to privacy in New Mexico and our suggestions and opinions about proposed Senate Bill S. 3418. Governor King's office has referred your letter to us for reply.

From constantly reading and hearing about government and private spying on individuals it is becoming extremely clear to most Americans that legislation such as you propose is becoming increasingly imperative in America.

New Mexico does not have a general statute relating to the individual's right to privacy. We have in certain areas found it necessary to impose restrictions on some forms of information gathering and release and to extend the area of privileged communications. (Copies of the applicable portions of these laws are attached.)

Section 67-33-25 N.M.S.A. 1953 Comp. prohibits private investigators from divulging information to one other than his employer, except as required by law, and prohibits the making of false reports.

New Mexico also adopted wiretap legislation, very similar to that on the Federal level, which provides penalties for unauthorized wiretapping. Section 40A–12–1 *supra.*

It is also illegal to Black-List employees. Section 40A–13–3.

The New Mexico legislature has deemed it desirable to protect the confidentiality of information furnished to and compiled by state agencies. Section 51–21–8, *supra,* (Corp. Commission) ; Section 72–13–25, *supra,* (Bureau of Revenue) ; Section 59–9–11.11 (Unemployment Compensation Commission).

New Mexico has also extended the area of privileged communication to, those engaged in or receiving treatment for drug abuse, Section 54–10–12, *supra,* 54–10–14, *supra,* to those engaged in drug research, Section 54–11–39, *supra,* to newspapermen, Section 20–1–12.1, to Psychotherapists, Section 20–4–504, to Clergymen, Section 20–4–506, to a person's vote, Section 20–4–507, and to trade secrets, 20–4–508.

Review of the copy of S. 3418 which you supplied reveals a well thought out comprehensive plan, a plan which is long overdue in this nation.

Under Title II Section 201(2)(A)(B) it would seem the provision prohibiting forced disclosure should be supplemented by a provision prohibiting a person's refusal to give such information from being held against him if he is applying for a job, or other positions.

Also under Title II(d)(5), if an individual challenges information against him we feel it should be clearly expressed that it is up to the data bank to prove the correctness of any information, its pertinency and the validity of any verification or such challenged information should be removed. It should be clear that it is not up to the individual to prove the information's incorrectness.

Under Title III Section 303, it would probably be desirable to provide minimum as well as maximum penalties. Under 'Exemptions', Title II Section 202, we feel, in light of developments over the last few years and recently, that exemptions such as specified here should be closely watched and controlled by Congress in order to prevent abuses which could forceably negate much of the act. Bitter experience has shown that information totally unrelated to national defense is often classified and protected under that heading.

There should be some review available to determine the validity of classifications made.

I hope we have been of assistance to you and that the enclosed information will prove helpful. If you have any further inquiry or specific questions, please contact: David L. Norvell, Attorney General, P.O. Box 2246, Sante Fe, N. Mex. 87501.

Sincerely,

FRANK MURRAY, *Law Clerk.*

Enclosures.

67–33–25. Prohibited acts.—A. Any licensee or officer, director, partner or manager of the licensee may divulge to any law enforcement officer or district attorney, attorney general or his representatives any information he may acquire as to any criminal offense, but he shall not divulge to any other person except as he may be required by law so to do any information acquired by him except at the direction of the employer or client from whom the information was obtained.

B. No licensee or officer, director, partner, manager or employee of a licensee shall knowlingly make any false report to his partner or client for whom information was being obtained.

C. No written report shall be submitted to a client except by the licensee, qualifying manager or a person authorized by one or either of them, and such person submitting the report shall exercise diligence in ascertaining whether or not the facts and information of such report are true and correct.

D. No licensee or officer, director, partner, manager or employee of private investigator shall use a badge in connection with the official activities with the licensee's business.

E. No licensee or officer, partner, director, manager or employee of a licensee shall use a title or wear a uniform, or use an insignia or use an identification card or make any statement with the intent to give an impression that he is connected in any way with the federal government, a state government or any political subdivision of a state government.

F. No licensee or officer, director, partner, manager or employee of a licensee shall enter any private building or portion thereof without the consent of the owner or of the person in possession thereof.

G. No private patrol licensee or officer, director, partner, manager or employee of a private patrol licensee shall use a badge except when engaged in guard or patrol work and while wearing a uniform.

H. No licensee shall appear as an assignee party in any proceeding involving claim and delivery, replevin or other possessory action, action for foreclosing a chattel mortgage, mechanic's lien, materialman's lien or any other lien.

40A-12-1. Interference with communications.—Interference with communications consists of knowlingly:

A. displacing, removing, injuring or destroying any radio station, T.V. tower, antenna or cable, telegraph or telephone line, wire, cable, pole or conduit belonging to another, or the material or property appurtenant thereto;

B. cutting, breaking, tapping or making any connection with any telegraph or telephone line, wire, cable or instrument belonging to another;

C. reading, hearing, interrupting, taking or copying any message, communication or report intended for another by telegraph or telephone without his consent;

D. preventing, obstructing or delaying the sending, transmitting, conveying or delivering in this state of any message, communication or report by or through telegraph or telephone; or

E. using any apparatus to do or cause to be done any of the acts hereinbefore mentioned or to aid, agree with, comply or conspire with any person to do, or permit or cause to be done any of the acts hereinbefore mentioned.

40A-12-1. Interference with communications—Exception.—Interference with communications consists of knowlingly:

A. to E. * * * [Same as parent volume.]

Whoever commits interference with communications is guilty of a misdemeanor, unless such interference with communications is done under a court order as provided in sections 40A-12-1.1 through 40A-12-1.10 NMSA 1953, or unless such interference with communications is done by an operator of a switchboard or an officer, employee or agent of any communication common carrier in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his services or to the protection of rights or property of the carrier of such communication.

40A-13-3. Black-listing.—Black-listing consists of an employer or his agent preventing or attempting to prevent a former employee from obtaining other employment.

Whoever commits black-listing is guilty of a misdemeanor.

Upon request, an employer may give an accurate report or honest opinion of the qualifications and the performance of a former employee. An employer is defined as any person employing labor or the agent of such person.

51-21-8. Commission to furnish forms—Release of information—Penalty.—A. The commission shall, upon application, furnish the necessary blanks in proper form and shall keep safely in its office all corporate reports alphabetically indexed.

B. Information obtained from reports filed pursuant to the provisions of the Corporate Reports Act [51-21-1 to 51-21-9] shall be made available to interested persons during proper hours, except that data contained in subsection B of section 51-21-2 New Mexico Statutes Annotated, 1953 Compilation shall not be released unless in statistical form classified to prevent identification of particular corporations.

C. All reports required under the Corporate Reports Act may be used as evidence at any trial or hearing of the commission.

D. All reports required under the Corporate Reports Act shall be made available to the bureau of revenue upon written request and the bureau shall be subject to the same restrictions upon revealing the information as are imposed by this section upon the corporation commission.

E. Any other state agency or department upon written request to the state corporation commission may examine reports filed with the corporation commission upon a showing that the corporate reports sought to be examined are germane to an investigation being conducted by the petitioning agency or department, and any information revealed is subject to subsection F of this section concerning the release of such information contrary to law by any person in the requesting agency or department.

F. Any person who releases information contrary to the provisions of this section is guilty of a misdemeanor and upon conviction shall be punished by a fine of not more than one thousand dollars ($1,000) nor less than one hundred dollars ($100) or by imprisonment in the county jail not more than ninety [90] days nor

less than thirty [30] days or by both fine and imprisonment in the discretion of the judge.

B. The status as of the last day of the preceding fiscal year of:

(1) the amount of capital stock, authorized, subscribed, actually issued and outstanding, the amount of capital stock paid up and the amount of treasury stock held by the corporation;

(2) the value and location of all property owned and used by the corporation in this state and the value and location of the property owned and used outside of this state;

(3) the total gross receipts derived from its property and business in this state and the total gross receipts from its property and business both within and without this state during the preceding year;

(4) a balance sheet of the financial condition of the corporation, indicating data prescribed by the commission; and

(5) if a foreign corporation doing business in this state as a railroad, telegraph or express company, the amount of its issued capital stock represented by its property and business in this state; and

72-13-25. Confidentiality of returns and other information.—It is unlawful for any employee of the bureau to reveal to any individual other than another employee of the bureau any information contained in the return of any taxpayer or any other information about any taxpayer acquired as a result of his employment by the bureau, except:

A. to an official representative of another state, upon the written request of the governor thereof, pursuant to the terms of a reciprocal agreement entered into with that state for exchange of such information;

B. to a representative of the secretary of the treasury or his delegate, pursuant to the terms of a reciprocal agreement entered into with the federal government for exchange of such information;

C. to a district court or the Supreme Court or a federal court in response to an order thereof in an action relating to taxes to which the state is a party and in which the information sought is material to the inquiry, in which case only that information may be required to be produced in court and admitted in evidence, and no more;

D. to the taxpayer himself or to his authorized representative;

E. in such manner, for statistical purposes, that the information revealed is not identified as applicable to any individual taxpayer;

F. with reference to any information concerning the tax on tobacco imposed by sections 72-14-1 through 72-14-17 NMSA 1953 and the tax on the severance of minerals contained in sections 72-18-1 through 72-18-51 NMSA 1953 to a committee of the legislature for a valid legislative purpose;

G. the names, taxpayers' identification numbers and addresses of registered gross receipts taxpayers in a municipality may be released to that municipality, whose employees are thereby subject to the penalty contained in section 72-13-88 NMSA 1953 if such information is revealed to individuals other than other employees of the municipality in question;

H. to the property appraisal department for use in auditing or assessing taxpayers. The property appraisal department and its employees are subject to the provisions of this section with respect to any information acquired from the bureau;

I. to the commissioner of public lands for use in auditing which pertains to rentals, royalties, fees and other payments due the state under land sale, land lease or other land use contracts. The commissioner of public lands and his employees are subject to the same provisions regarding confidentiality of information as employees of the bureau;

J. the bureau shall furnish, upon request by the central parent locator unit of the health and social services department, the last known address with date of all names certified to the bureau as being absent parents of children receiving public financial assistance. The central parent locator unit personnel shall use such information only for the purpose of enforcing the support liability of such absent parents and shall not use the information or disclose it for any other purpose. The central parent locator unit and its employees are subject to the provisions of this section with respect to any information acquired from the bureau;

K. with respect to the tax on gasoline imposed by the Gasoline Tax Act [72-27-1 to 72-27-15], the bureau shall make available for public inspection at monthly intervals a report covering the amount and gallonage of gasoline imported, exported, sold and used, including tax exempt sales to the federal gov-

ernment reported or upon which the gasoline tax was paid, together with a tabulation of taxes received from each distributor in the state of New Mexico;

L. the returns required of gasoline wholesalers under the Gasoline Tax Act may be released upon request, to municipalities and counties whose employees or agent are thereby subject to the penalty contained in section 72-13-88 NMSA 1953 if such information is revealed to individuals other than other employees of the municipality or county in question; and

M. the bureau shall answer all inquiries concerning whether a person is or is not a registered taxpayer.

History: Laws 1965, ch. 248, § 13; 1969, ch. 8, § 1; 1970, ch. 16, § 1; 1971, ch. 276, § 5.

59-9-11.11. Disclosure of information—Penalty.—A. Information obtained from any employing unit or individual pursuant to administration of the Unemployment Compensation Law [59-9-1 to 59-9-29] and determinations as to benefit rights of any individual are confidential and shall not be disclosed or be open to public inspection in any manner revealing the individual's or employing unit's identity, except that such information may be made available under such restrictions as the commission may prescribe to:

(1) Any agency of this or any other state or any federal agency charged with administration of an unemployment compensation law or maintenance of a system of public employment offices;

(2) The United States treasury department bureau of internal revenue; and

(3) The income tax division, school tax division and compensating tax division of the New Mexico bureau of revenue.

Any claimant or his legal representative shall be supplied with information from the records of the commission to the extent necessary for proper presentation of his claim in any proceeding under the Unemployment Compensation Law. Information obtained in connection with administration of the employment service may be made available to persons or agencies for purposes appropriate to the operation of a public employment service.

Upon request, the commission shall furnish to any agency of the United States charged with administration of public works or assistance through public employment, and may furnish to any state agency similarly charged, the name, address, ordinary occupation and employment status of each recipient of benefits and the recipient's rights to further benefits under the Unemployment Compensation Law. The commission may request the comptroller of currency of the United States to cause an examination of the correctness of any return or report of any national banking association rendered pursuant to the Unemployment Compensation Law and in connection with such request may transmit any report or return as provided in section 1606(c) of the Internal Revenue Code, 26 U.S.C. § 1606(c).

B. Any employee or member of an appeal tribunal of the commission or employee of the commission who, in violation of the provisions of this section, makes any disclosure of information obtained from any employing unit or individual in the administration of the Unemployment Compensation Law or any person who has obtained any list of applicants for work or of claimants or recipients of benefits under the Unemployment Compensation Law who uses or permits the use of such list for any political purpose, shall be fined not less than twenty dollars ($20.00) nor more than two hundred dollars ($200), or imprisoned for not more than ninety [90] days, or both.

History: C. 1953, § 59-9-11.11 enacted by Laws 1959, ch. 321, § 12; Laws 1961, ch. 201, § 1.

Title of Act.

An act providing that information in the records of the employment security commission may be made available to the school tax division and the compensating tax division of the bureau of revenue; amending section 59-9-11.11 New Mexico Statutes Annotated, 1953 Compilation (being Laws 1959, chapter 321, section 12).—Laws 1961, ch. 201.

Amendment.

The 1961 amendment inserted "school tax division and compensating tax division" in subdivision (3) of subsection A.

54-10-12. Confidential nature of records and information.—The agency shall promulgate regulations to safeguard the confidential nature of records of and information about the recipients of services provided under the Drug Abuse Act

[54-10-1 to 54-10-12]. The regulations shall require that the local eligible entities develop and include in any application for financial participation adequate provisions for safeguarding confidential information. Unless the application and contract cover this subject adequately they shall not be approved. The agency's regulations may provide for disclosure of confidential information to professional personnel providing direct services to a recipient and to other appropriate service agencies.

History: Laws 1971, ch. 244, § 12.

54-10-14. Capability to submit to drug abuse treatment—Liability for expenses—Confidentiality of records.—A. Any person, regardless of age, may submit himself for drug abuse treatment to any licensed physician, public or private hospital, clinic supervised by a licensed physician or any institution or facility maintained in whole or in part by state or federal funds.

B. No parent or other legal guardian shall be liable for payment of drug abuse treatment expenses if the treatment was made without his written consent.

C. The treating facility or person shall keep such records on drug abuse treatment as are necessary or required by law. The records shall be confidential, and may be used only for rehabilitation, research, statistical and medical purposes. No such records or any information contained in them shall be discoverable by the state in any criminal prosecution.

54-11-39. Research—Confidentiality.—A. The board shall encourage research on misuse and abuse of controlled substances. In connection with the research, and in furtherance of the enforcement of the Controlled Substances Act, it may register public agencies, institutions of higher education, and private organizations or individuals for the purpose of conducting research, demonstrations or special projects which bear directly on misuse and abuse of controlled substances.

B. The board may authorize persons engaged in research on the use and effects of controlled substances to withhold the names and other identifying characteristics of individuals who are subjects of the research. Persons who obtain this authorization are not compelled in any civil, criminal, administrative, legislative or other proceeding to identify the individuals who are the subjects of research for which the authorization was obtained.

C. The board may authorize the possession and distribution of controlled substances by persons engaged in research. Such authorization shall contain the conditions and terms of the research to be conducted. Persons who obtain this authorization are exempt from state prosecution for possession and distribution of controlled substances to the extent of the authorization.

D. A practitioner engaged in medical practice or research shall not be required to furnish the name or identity of a patient or research subject to the board, nor may he be compelled in any state or local civil, criminal, administrative,. legislative or other proceedings to furnish the name or identity of an individual that the practitioner is obligated to keep confidential.

History: Laws 1972, ch. 84, § 39.

Savings Clause.

Section 40 of ch. 84, Laws 1972 read: "A. Prosecution for any violation of law occurring prior to the effective date of the Controlled Substances Act is not affected by the Controlled Substances Act. If the offense being prosecuted is similar to one set out in sections 20 through 25 of the Controlled Substances Act, then the penalties under sections 20 through 25 apply if they are less than those under prior law.

"B. Civil seizures or forfeitures and injunctive proceedings commenced prior to the effective date of the Controlled Substances Act are not affected by the Controlled Substances Act.

"C. All administrative proceedings pending under prior laws, which are superseded by the Controlled Substances Act, shall be continued and brought to a final determination in accord with the laws and regulations in effect prior to the effective date of the Controlled Substances Act.

"D. The board shall initially permit persons to register who own or operate any establishment engaged in the manufacture, distribution or dispensing of any controlled substance prior to the effective date of the Controlled Substances Act and who are registered or licensed by the state.

"E. The Controlled Subsances Act applies to violations of law, seizures and forfeiture, injunctive proceedings, administrative proceedings and investigations which occur following its effective date."

Continuation of Rules.

Section 41 of ch. 84, Laws 1972 read: "Any orders and regulations affected by the Controlled Substances Act in effect on the effective date of the Controlled Substances Act, and not in conflict with it, continue in effect until modified, superseded or repealed."

Separability Clause.

Section 42 of ch. 84, Laws 1972 read: "If any part or application of the Controlled Substances Act is held invalid, the remainder or its application to other situations or persons shall not be affected."

20-1-12. Privileged communications.—A. No husband shall be compelled to disclose any communication made by his wife during the marriage, and no wife shall be compelled to disclose any communication made to her by her husband during the marriage.

B. An attorney cannot, without the consent of his client, be examined as to any communication made by the client to him, or his advice given thereon in the course of professional employment; nor can an attorney's secretary, stenographer, or clerk be examined, without the consent of his employer, concerning any fact the knowledge of which has been acquired in such capacity.

C. In the courts of the state, no certified public accountant or public accountant shall be permitted to disclose information obtained in the conduct of any examination, audit or other investigation made in a professional capacity, or which may have been disclosed to said accountant by a client, without the consent in writing of such client or his, her or its successors or legal representatives.

D. If a person offers himself as a witness and voluntarily testifies with reference to the communications specified in this section, that is a consent to the examination of the person to whom the communications were made as above provided.

Title of Act.

An act relating to evidence in court proceedings; amending certain sections of the NMSA 1953; repealing certain sections of the NMSA 1953.—Laws 1973, ch. 223.

Amendments.

The 1973 amendment deleted former subsections (c) and (d) shown in the parent volume, designating former subsections (e) and (f) as C and D and made minor changes in phraseology and style.

20-1-12.1. News sources and information—Mandatory disclosure prohibited—Definitions—Special procedure for prevention of injustice issue.—A. Unless disclosure be essential to prevent injustice, no journalist or newscaster, or working associates of a journalist or newscaster, shall be required to disclose before any proceeding or authority, either:

(1) the source of any published or unpublished information obtained in the gathering, receiving or processing of information for any medium of communication to the public; or

(2) any unpublished information obtained or prepared in gathering, receiving or processing of information for any medium of communication to the public.

B. For the purpose of this act:

(1) "proceeding or authority" includes any proceeding or investigation before, or by, any legislative, judicial, executive or administrative body or person;

(2) "medium of communication" means any newspaper, magazine, press association, news service, wire service, news or feature syndicate, broadcast or television station or network, or cable television system;

(3) "information" means any written, oral or pictorial news or other material;

(4) "published information" means any information disseminated to the public by the person from whom disclosure is sought;

(5) "unpublished information" includes information not disseminated to the public by the person from whom disclosure is sought, whether or not related information has been disseminated, and includes but is not limited to, all notes, news copy, outtakes, photographs, films, recording tapes or other data of whatever sort not disseminated to the public through a medium of communication;

(6) "processing" includes compiling, storing and editing of information;

(7) "journalist" means any person who, for gain is engaged in gathering, preparing, editing, analyzing or commenting on news for a newspaper, magazine, news agency, news or feature syndicate, press association or wire service ,or who was so engaged at the time a source or information was procured;

(8) "newscaster" means any person who, for gain is engaged in gathering, preparing, editing, analyzing, commenting on or broadcasting news for radio or television transmission, or who was so engaged at the time a source or information was procured; and

20–4–502. Rule 502—Required reports privileged by statute.

A person, corporation, association, or other organization or entity, either public or private, making a return or report required by law to be made has a privilege to refuse to disclose and to prevent any other person from disclosing the return or report, if the law requiring it to be made so provides. A public officer or agency to whom a return or report is requied by law to be made has a privilege to refuse to disclose the return or report if the law requiring it to be made so provides. No privilege exists under this rule in actions involving perjury, false statements, fraud in the return or report, or other failure to comply with the law in question.

20–4–503. Rule 503—Lawyer-client privilege.

(a) DEFINITIONS. As used in this rule:

(1) A "client" is a person, public officer, or corporation, association, or other organization or entity, either public or private, who is rendered professional legal services by a lawyer, or who consults a lawyer or a representative of a lawyer with a view to obtaining professional legal services from him.

(2) A "lawyer" is a person authorized, or reasonably believed by the client to be authorized, to practice law in any state or nation.

(3) A "representative of the lawyer" is one employed to assist the lawyer in the rendition of professional legal services.

(4) A communication is "confidential" if not intended to be disclosed to third persons other than those to whom disclosure is in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication.

(b) GENERAL RULE OF PRIVILEGE. A client has a privilege to refuse to disclose and to prevent any other person fom disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client, (1) between himself or his representative and his lawyer or his lawyer's representative, or (2) between his lawyer and the lawyer's representative, or (3) by him or his lawyer to a lawyer representing another in a matter of common interest, or (4) between representatives of the client or between the client and a representative of the client, or (5) between lawyers representing the client.

(c) WHO MAY CLAIM THE PRIVILEGE. The privilege may be claimed by the client, his guardian or conservator, the personal representative of a deceased client, or the successor, trustee, or similar representative of a corporation, association, or other organization, whether or not in existence. The person who was the lawyer at the time of the communication may claim the privilege but only on behalf of the client. His authority to do so is presumed in the absence of evidence to the contrary.

(d) EXCEPTIONS.—There is no privilege under this rule:

(1) Furtherance of Crime or Fraud. If the services of the lawyer were sought or obtained to enable or aid anyone to commit or plan to commit what the client knew or reasonably should have known to be a crime or fraud; or

(2) Claimants Through Same Deceased Client. As to a communication relevant to an issue between parties who claim through the same deceased client, regardless of whether the claims are by testate or intestate succession or by inter vivos transaction; or

(3) Breach of Duty by Lawyer or Client. As to a communication relevant to an issue of breach of duty by the lawyer to his client or by the client to his lawyer; or

(4) Document Attested by Lawyer. As to a communication relevant to an issue concerning an attested document to which the lawyer is an attesting witness; or

(5) Joint Clients. As to a communication relevant to a matter of common interest between two or more clients if the communication was made by any of them to a lawyer retained or consulted in common, when offered in an action between any of the clients.

Cross-References.

Attorney-client privilege, 20–1–12.

20–4–504. Rule 504—Psychotherapist-patient privilege.

(a) DEFINITIONS.

(1) A "patient" is a person who consults or is examined or interviewed by a psychotherapist.

(2) A "psychotherapist" is (A) a person authorized to practice medicine in any state or nation, or reasonably believed by the patient so to be, while engaged in the diagnosis or treatment of a mental or emotional condition, including drug addiction, or (B) a person licensed or certified as a psychologist under the laws of any state or nation, while similarly engaged.

(3) A communication is "confidential" if not intended to be disclosed to third persons other than those present to further the interest of the patient in the consultation, examination, or interview, or persons reasonably necessary for the transmission of the communication, or persons who are participating in the diagnosis and treatment under the direction of the psychotherapist, including members of the patient's family.

(b) General Rule of Privilege. A patient has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications, made for the purposes of diagnosis or treatment of his mental or emotional condition, including drug addiction, among himself, his psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist, including members of the patient's family.

(c) Who May Claim the Privilege. The privilege may be claimed by the patient, by his guardian or conservator, or by the personal representative of a deceased patient. The person who was the psychotherapist may claim the privilege but only on behalf of the patient. His authority so to do is presumed in the absence of evidence to the contrary.

(d) Exceptions.

(1) Proceedings for Hospitalization. There is no privilege under the rule for communications relevant to an issue in proceedings to hospitalize the patient for mental illness, if the psychotherapist in the course of diagnosis or treatment has determined that the patient is in need of hospitalization.

(2) Examination by Order of Judge. If the judge orders an examination of the mental or emotional condition of the patient, communications made in the course thereof are not privileged under this rule with respect to the particular purpose for which the examination is ordered unless the judge orders otherwise.

(3) Condition an Element of Claim or Defense. There is no privilege under this rule as to communications relevant to an issue of the mental or emotional condition of the patient in any proceeding in which he relies upon the condition as an element of his claim or defense, or, after the patient's death, in any proceeding in which any party relies upon the condition as an element of his claim or defense.

20–4–505. Rule 505—Husband-wife privilege.

(a) General Rule of Privilege. An accused spouse in a criminal proceeding has a privilege to prevent the other spouse from testifying against the accused.

(b) Who May Claim the Privilege. The privilege may be claimed by the accused or by the other spouse. The authority of the other spouse to do so is presumed in the absence of evidence to the contrary.

(c) Exceptions. There is no privilege under this rule (1) in proceedings in which one spouse is charged with a crime against the person or property of the other spouse or of a child of either, or with a crime against the person or property of a third person committed in the course of committing a crime against the other spouse, or (2) as to matters occurring prior to the marriage.

Cross-References.

Husband and wife, privileged communications, 20–1–12.

20–4–506. Rule 506—Communications to clergymen.

(a) Definitions. As used in this rule:

(1) A "clergyman" is a minister, priest, rabbi, or other similar functionary of a religious organization, or an individual reasonably believed so to be by the person consulting him.

(2) A communication is "confidential" if made privately and not intended for further disclosure except to other persons present in furtherance of the purpose of the communication.

(b) General Rule of Privilege. A person has a privilege to refuse to disclose and to prevent another from disclosing a confidential communication by the person to a clergyman in his professional character as spiritual adviser.

(c) Who May Claim the Privilege. The privilege may be claimed by the person, by his guardian or conservator, or by his personal representative if he is

deceased. The clergyman may claim the privilege on behalf of the person. His authority so to do is presumed in the absence of evidence to the contrary.

20–4–507. Rule 507—Political vote.

Every person has a privilege to refuse to disclose the tenor of his vote at a political election conducted by secret ballot unless the vote was cast illegally.

20–4–508. Rule 508—Trade secrets.

A person has a privilege, which may be claimed by him or his agent or employee, to refuse to disclose and to prevent other persons from disclosing a trade secret owned by him, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice. When disclosure is directed, the judge shall take such protective measure as the interests of the holder of the privilege and of the parties and the furtherance of justice may require.

20–4–509.—Rules 509 (Reserved).

20–4–510. Rule 510—Identity of informer.

(a) RULE OF PRIVILEGE. The United States or a state or subdivision thereof has a privilege to refuse to disclose the identity of a person who has furnished information relating to or assisting in an investigation of a possible violation of law to a law enforcement officer or member of a legislative committee or its staff conducting an investigation.

(b) WHO MAY CLAIM. The privilege may be claimed by an appropriate representative of the United States or a state or subdivision thereof, except that in criminal cases the privilege shall not be allowed if the state objects.

(c) EXCEPTIONS:

(1) Voluntary Disclosure; Informer a Witness. No privilege exists under this rule if the identity of the informer or his interest in the subject matter of his communication has been disclosed to those who would have cause to resent the communication by a holder of the privilege or by the informer's own action, or if the informer appears as a witness for the state.

(2) Testimony on Merits. If it appears from the evidence in the case or from other showing by a party that an informer will be able to give testimony that is relevant and helpful to the defense of an accused, or is necessary to a fair determination of the issue of guilt or innocence in a criminal case or of a material issue on the merits in a civil case to which the state or a subdivision thereof is a party, and the state or subdivision thereof invokes the privilege, the judge shall give the state or subdivision thereof an opportunity to show in camera facts relevant to determining whether the informer can, in fact, supply that testimony. The showing will ordinarily be in the form of affidavits, but the judge may direct that testimony be taken if he finds that the matter cannot be resolved satisfactorily upon affidavit. If the judge finds that there is a reasonable probability that the informer can give the testimony, and the state or subdivision thereof elects not to disclose his identity, the judge on motion of the defendant in a criminal case shall dismiss the charges to which the testimony would relate, and the judge may do so on his own motion. In civil cases, he may make any order that justice requires. Evidence submitted to the judge shall be sealed and preserved to be made available to the appellate court in the event of an appeal, and the contents shall not otherwise be revealed without an order of the court. All counsel shall be permitted to be present at any stage at which counsel for any party is permitted to be present.

(3) Legality of Obtaining Evidence. If information from an informer is relied upon to establish the legality of the means by which evidence was obtained and the judge is not satisfied that the information was received from an informer reasonably believed to be reliable or credible, he may require the identity of the informer to be disclosed. The judge may permit the disclosure to be made in camera or make any other order which justice requires. All counsel concerned with the issue of legality shall be permitted to be present at every stage at which any counsel is permitted to be present. If disclosure of the identity of the informer is made in camera, the record thereof shall be sealed and preserved to be made available to the appellate court in the event of an appeal, and the contents shall not otherwise be revealed except by order of a court having jurisdiction.

20–4–511. Rule 511—Waiver of privilege by voluntary disclosure.

A person upon whom these rules confer a privilege against disclosure of the confidential matter or communication waives the privilege if he or his predecessor while holder of the privilege voluntarily discloses or consents to disclosure of any significant part of the matter or communication. This rule does not apply if the disclosure is itself a privileged communication.

20–4–512. Rule 512—Privileged matter disclosed under compulsion or without opportunity to claim privilege.

Evidence of a statement or other disclosure of privileged matter is not admissible against the holder of the privilege if the disclosure was (a) compelled erroneously or (b) made without opportunity to claim the privilege.

20–4–513. Rule 513—Comment upon or inference from claim of privilege; instruction.

(a) COMMENT OF INFERENCE NOT PERMITTED. The claim of a privilege, whether in the present proceeding or upon a prior occasion, is not a proper subject of comment by judge or counsel. No inference may be drawn therefrom.

(b) CLAIMING PRIVILEGE WITHOUT KNOWLEDGE OF JURY. In jury cases, proceedings shall be conducted, to the extent practicable, so as to facilitate the making of claims of privilege without the knowledge of the jury.

(c) JURY INSTRUCTION. Upon request, any party against whom the jury might draw an adverse inference from a claim of privilege is entitled to an instruction that no inference may be drawn therefrom.

VI. WITNESSES

20–4–601. Rule 601—General rule of competency.

Every person is competent to be a witness except as otherwise provided in these rules.

20–4–602. Rule 602—Lack of personal knowledge.

A witness may not testify to a matter unless evidence is introduced sufficient to support a finding that he has personal knowledge of the matter. Evidence to prove personal knowledge may, but need not, consist of the testimony of the witness himself. This rule is subject to the provisions of Rule 703 [20–4–703], relating to opinion testimony by expert witnesses.

20–4–603. Rule 603—Oath or affirmation.

Before testifying, every witness shall be required to declare that he will testify truthfully, by oath or affirmation administered in a form calculated to awaken his conscience and impress his mind with his duty to do so.

Cross-References. Rules of Criminal Procedure, 41–23–48.

Rules of Civil Procedure, affirmation in lieu of oath, 21–1–1 (43) (d).

20–4–604. Rule 604—Interpreters.

An interpreter is subject to the provisions of these rules relating to qualification as an expert and the administration of an oath or affirmation that he will make a true translation.

STATE OF NEW YORK

DEPARTMENT OF LAW,
Albany, N.Y., July 10, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Senate Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: This will acknowledge your letter of June 25 in which you seek my comments with respect to S. 3418 concerning individual privacy, establishment of a Federal Privacy Board and management information systems.

The subject matter is of great interest and concern to me and to the people of the State of New York. Your request will be given very careful consideration with a view towards a response in substance as soon as possible.

I am enclosing for your information Chapters 407 and 408 of the Laws of 1973, enacted at my request in New York State, which chapters relate to the problems you discussed in your correspondence with respect to billing practices and consumer credit.

Sincerely,

LOUIS J. LEFKOWITZ,
Attorney General.

Enclosure.

LAWS OF NEW YORK.—By Authority

CHAPTER 407

AN ACT to amend the general business law, in relation to creditor billing errors

Became a law June 5, 1973, with the approval of the Governor. Passed by a majority vote, three-fifths being present

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Article thirty and sections six hundred and six hundred one of the general business law are hereby renumbered to be, respectively, article forty and sections nine hundred and nine hundred one of such law.

§ 2. Such law is hereby amended by inserting therein a new article, to be article thirty-four, to read as follows:

ARTICLE 34

CREDITOR BILLING ERRORS

Section 701. Definitions.
702. Application.
703. Notice of error and response.
704. Permissible procedures by creditor.
705. Statement to contain instructions for notification of error.
706. Notice to consumer of this act.
707. Penalties.

§ 701. Definitions. Whenever used in this article:

1. "Consumer" means a natural person.

2. "Creditor" means a person, partnership, corporation, association or other entity who, in the ordinary course of business, regularly extends consumer credit.

3. "Consumer credit" means credit extended to a consumer, primarily for personal, family or household purposes, pursuant to a plan under which the creditor may permit the consumer to make purchases or obtain loans, from time to time, directly from the creditor or indirectly by use of a credit card, check or other device, as the plan may provide.

4. "Billing error" means the initial occurrence of an error by omission or commission by the creditor in a billing statement given to the consumer by the creditor in (a) posting any debit or credit

EXPLANATION — Matter in *italics* is new; matter in brackets [ ] is old law to be omitted.

or (b) the computation of any amount or (c) any similar error of an accounting nature.

§ 702. Application. This chapter shall not apply to statements of accounts rendered to customers by public utilities whose billing practices are subject to the jurisdiction and regulation of the public service commission.

§ 703. Notice of error and response. If a creditor, having transmitted to a consumer a statement of the consumer's account, receives from the consumer at an address designated therefor by the creditor in accordance with section seven hundred five of this act, within thirty days of the mailing of said statement, a written notice, on a document other than a document provided by the creditor to accompany payment, by registered or certified mail, return receipt requested, setting forth sufficient information to enable the creditor to identify the consumer and the account, the amount and transaction shown in the statement which the consumer in good faith believes to be a billing error, and the facts providing the basis for the consumer's belief that the statement is in error; the creditor shall:

1. Not later than thirty days after receipt of the notice, mail a written acknowledgment to the consumer; and

2. Not later than ninety days after receipt of the notice and prior to taking any action to collect the amount believed by the consumer to be a billing error, (a) make appropriate corrections in the account of the consumer and mail to the consumer a written notice stating that the amount believed to be in error has been corrected and will be shown on the next statement mailed to the consumer or (b) send a written notice to the consumer setting forth the reasons why the creditor believes the account of the consumer was correctly shown in the statement; and

3. Not communicate unfavorable credit information concerning the consumer to any person, including but not limited to credit bureaus or credit reporting agencies, based upon the consumer's failure to pay the amount believed by him to be a billing error, until the creditor has complied with this section.

§ 704. Permissible procedures by creditor. Notwithstanding the receipt by a creditor of a notice from a consumer as described in section seven hundred three of this act, a creditor may, subject to the provisions of section seven hundred seven of this act, transmit statements of account to the consumer which include an amount believed by the consumer to be a billing error, and the creditor, further, may undertake collection procedures not attributable to such consumer's failure to pay, nor directed at, such disputed amount.

§ 705. Statement to contain instructions for notification of error. Every statement of account rendered by a creditor to a consumer shall include the address to be used by the consumer in making inquiries concerning his statement.

§ 706. Notice to consumer of this act. Not later than sixty days after the effective date of this act, a creditor shall send to each consumer, whose account was in existence on the effective date of this act, and with the first billing statement on any consumer credit plan issued or offered to a new consumer after the effective date of this act and upon each subsequent renewal of a consumer's account a written notice (by any means reasonably assuring the receipt thereof by the consumer) which describes the procedures to be followed under section seven hundred three of this act.

§ 707. Penalties. Any creditor, having received a notice from a consumer as provided in section seven hundred three of this act, who fails to comply with the requirements of that section:

1. If such an amount is not in fact a billing error, forfeits any rights to collect from the consumer any finance charge or other charge imposed by the creditor in connection with the amount so specified, from the date of the mailing of such notice to the date the creditor complies with section seven hundred three of this act; and

2. If such amount is in fact a billing error, is liable to the consumer in an amount equal to the sum of:

(a) the actual damages sustained by the consumer as a result of the failure of the creditor to comply with such section;

(b) twice the amount of the billing error shown in the statement of the consumer's account except that liability under this paragraph shall not be greater than one hundred dollars; and (c) in the case of any successful action to enforce the foregoing liability, the costs of the action together with a reasonable attorney's fee as determined by the court.

3. If such amount is in fact a billing error but the creditor shows by a preponderance of evidence that the violation was not intentional and resulted from bona fide error made despite the maintenance of procedures reasonably adopted to avoid any such error, the creditor shall be liable to the consumer only to the extent of the actual damages sustained by the consumer as a result of the failure of the creditor to comply with such section and the costs of any action brought to enforce collection of such erroneous bill together with a reasonable attorney's fee as determined by the court.

§ 3. This act shall take effect on the first day of November next succeeding the date on which it shall have become a law.

STATE OF NEW YORK }
Department of State } *ss:*

I have compared the preceding with the original law on file in this office, and do hereby certify that the same is a correct transcript therefrom and of the whole of said original law.

JOHN P. LOMENZO
Secretary of State

LAWS OF NEW YORK.—By Authority

CHAPTER 408

AN ACT to amend the general business law, in relation to giving notice to consumer by creditor of procedure in creditor billing

Became a law June 5, 1973, with the approval of the Governor. Passed by a majority vote, three-fifths being present

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Section seven hundred six of the general business law, as added by a chapter of the laws of nineteen hundred seventy-three entitled "An Act to amend the general business law, in relation to creditor billing errors", is hereby amended to read as follows:

§ 706. Notice to consumer of this act. Not later than sixty days after the effective date of this act, a creditor shall send to each consumer, whose account was in existence on the effective date of this act, and with *or before* the first billing statement on any consumer credit plan issued or offered to a new consumer after the effective date of this act and upon each subsequent renewal of a consumer's account a written notice (by any means reasonably assuring the receipt thereof by the consumer) which describes the procedures to be followed under section seven hundred three of this act. *Provided, however, that with respect to an existing account on which there is no debit or credit balance on the effective date of this act, a creditor shall have the option of sending such notice with or before the first billing statement issued on such account after the effective date of this act.*

§ 2. This act shall take effect on the first day of November next succeeding the date on which it shall have become a law.

EXPLANATION — Matter in *italics* is new; matter in brackets [ ] is old law to be omitted.

STATE OF NEW YORK }
Department of State } *ss:*

I have compared the preceding with the original law on file in this office, and do hereby certify that the same is a correct transcript therefrom and of the whole of said original law.

JOHN P. LOMENZO
Secretary of State

STATE OF NORTH DAKOTA

ALLEN I. OLSON, ATTORNEY GENERAL,
Bismarck, N. Dak., August 1, 1974.

Re: S. 3418, sponsored by Senators Ervin, Muskie, and Percy.

Senator SAM J. ERVIN JR.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: Your inquiry dated June 25, 1974, concerning our assessment and judgment of the captioned bill can now be answered with candor and with meaningful suggestion for the reason that this writer has completed a working draft of our new rules and guidelines governing the security, privacy, completeness and correctness of information in our also new Criminal Offender Records System, since receipt of your letter in our office.

We will be glad to send copy of our newly drawn rules and guidelines if you and your committee would see a need for it. However, as your committee and you, we have been extremely patient and careful in our State so as to make our paramount concern the insuring of fairness, accuracy and privacy in criminal offender records, with secondary consideration for right to challenge inaccurate or incomplete records by the aggrieved individual, physical security of records and equipment, strictly controlled dissemination of criminal offender records to qualified criminal justice agencies and limited dissemination for analytical and research purposes.

We will have an absolute prohibition against collection or dissemination of raw intelligence data (we do not like computer banks filled row on row with senseless and trivial information about citizens, hanging like the Sword of Damocles over people, ready to fall and literally destroy a lifetime-long and carefully built reputation by one unwarranted innuendo from a computer, programmed into the machine we know not when, by whom, or even why). Our rules and guidelines also contain sanctions, under both civil and criminal law for misuse or violation of any of the proposed rules.

If my testimony would be required by your committee, I would be available on reasonable prior notice. I certainly do not consider myself an expert in the criminal offender records field, but my long experience as a prosecutor and as liaison officer for the North Dakota Attorney General's Office convinces me that your bill is not overly harsh or drastic or revoluntionary. It simply is a bill that will do the job and seal up the unconscionable and unwarranted leakage and exchange of highly personal information gathered under the guise of criminal offender record information, then freely and callously traded, bartered, and sold for profit over and over again.

Your bill will help insure to every American in generations to come that Big Brother does not need to know more about us as individuals than is necessary to govern and guide us as free men; and not as the pathetic targets of every muckraking and frustrated demagogue who relies on what "his" computer "has on" the citizen.

We commend your committee for your efforts and concern.

Sincerely,

CONRAD J. ZIEGLER,
Special Assistant Attorney General.

STATE OF OHIO

OFFICE OF THE ATTORNEY GENERAL,
Columbus, Ohio, July 19, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: This is in reference to your letter dated June 25, 1974 in which you enclosed Senate Bill #3418 and requested my comments on this and other federal legislation.

Please be advised that this Office is deeply involved in the computerization of the Criminal Justice System in Ohio. The Bureau of Criminal Identification and Investigation, which is a section within this Office, has primary responsibility for the design, development and operation of Criminal Histories, Offender Track-

ing System and the Uniform Crime Reports within the Criminal Justice Information System (CJIS).

The CJIS concept and design is being managed by a CJIS Steering Committee made up of representatives from law enforcement, corrections, courts, the State Data Center, regional planning units and this Office.

A separate sub-committee titled, "Security and Privacy" reviews all matters concerning the design and implementation as it related to individual privacy and systems security. It reviews all proposed, pending and existing legislation. It relies on technical memoranda and the Law Enforcement Assistance Administration (LEAA) in making its recommendations to the Steering Committee as a whole.

System design in the State of Ohio is now well advanced. Implementation is projected for September, 1975. Therefore, the Steering Committee and this Office are most interested in monitoring and commenting on any legislation which impacts that system.

Regarding the proposed legislation now before the United States Congress, I would make the following observations: This Office and the Steering Committee completely agree that any computerization of criminal records and its attending data must respect the individual's constitutional right to privacy.

In addition, this legislation should recognize law enforcement's responsibility to insure that while it is performing its tasks, it balances its responsibility with the individual's right to privacy.

Furthermore, the legislation should allow the states to take maximum advantage of existing and future technical advancements in this area.

The legislation should also be defined in a very careful manner to insure that its provisions are not technically or financially impractical. In order to accomplish this, the legislation should continue to seek advice and imput from law enforcement and computer experts during its drafting.

Any legislation should also allow for and recognize the advantage in the interface wih existing state systems and state legislation. Careful consideration should be given to the technical memoranda produced by LEAA and Project SEARCH.

In regard to Senate Bill #3418, 3633, the Hruska Bill and others which this Office has reviewed, I would make the following observations: If legislation will create a federal Privacy Control Board, it should be managed by law enforcement experts and technicians who are familiar with the problems and practicalities. This management should be subject to legal review, possibly by the Attorney General.

In addition, if the individual states have set up the machinery and legislation for the same or stricter review, the federal government should leave to those individual states a degree of independence in designing their systems.

Finally, it is recommended that there be closer coordination with the federal agencies which are involved in this matter. In this regard, it is suggested that those individuals in LEAA who are responsible for granting funds to the states for CJIS projects be constantly consulted since they, through their conditions to grant awards, have already "legislated" certain restrictions on states.

In conclusion, let me express my appreciation to you for allowing me and my staff to comment on this matter. As future legislation and testimony becomes available, this Office is willing and able to participate in this dialogue. Should you desire this Office's view on any specific technical or legal provision within any specific piece of legislation, please do not hesitate to contact me.

Again, thank you for your consideration in this matter, and please be assured of this Office's cooperation in all matters of mutual concern.

Very truly yours,

WILLIAM J. BROWN,
Attorney General.

OHIO DEPARTMENT OF ADMINISTRATIVE SERVICES,
OFFICE OF THE DIRECTOR,
Columbus, Ohio, July 25, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: On behalf of Governor John J. Gilligan, I am pleased to reply to your letter of June 25, 1974. Ohio State Government has been concerning with the "right of privacy" and the Department of Administrative Serv-

ices has implemented a policy of prohibiting the exchange of personal information except when such exchange either (1) is required by law, (2) is the result of an existing contract, or (3) will benefit the welfare of the citizens of Ohio.

Our experience has shown that the regulation of the exchange of information quite often has to be dealt with on a case by case basis; this is particularly true in the use of mailing lists. The following examples are included to illustrate the problem:

The legislature has required that Ohio pharmacists, in order to renew their licenses, complete certain continuing education programs. Ohio State University and other institutions have established programs which will enable pharmacists to fill this requirement. So that pharmacists can be informed of these programs, we have allowed accredited institutions to use our mailing list of licensed pharmacists.

The Department of Public Welfare has used files of dentists, doctors, pharmacists and nurses in order to validate its file of Medicaid Providers.

Mailing lists are not being sold where the purpose is direct mailings to individuals of promotional material.

Similarly, our experience suggests that stringent restriction on the use of Social Security Numbers would play havoc with beneficial and justifiable uses of this number which are already entente in both the private and public sectors. The Social Security Number is a tool; the real issues are protection of the confidentiality of the information which is with it and the use of that information.

In addition, our experience indicates that there ought to be a board which could address the unique cases which will have to be considered under this kind of regulation. As I pointed out above, we have had to take a flexible approach in our regulation of mailing lists. We feel that it would be impossible for the law to deal with privacy safeguards in the detail needed for flexibility. Furthermore, placing the responsibility for administering this law in an existing agency would most likely mean that the regulator would have to regulate himself.

As far as which systems should be covered by this legislation, I would like to make two points:

1. The legislation should cover both criminal justice and non-criminal justice systems. The need for legislation is especially pressing in the criminal justice area and, because of this, criminal justice systems should not be exempted. Making this legislation apply to criminal justice information should not, however, preclude legislation which specifically applies to criminal justice. That area may require additional safeguards.

2. Legislation to cover the private sector is needed at the Federal level to cover the private sector. It is impossible for the states to write bills effectively covering those organizations which are involved in interstate commerce.

Turning to S. 3418, I would like to make a few comments:

1. We applaud the approach taken in this bill, especially the following: a. The Federal Privacy Board; b. The fact that all information systems are covered; c. The completeness of the safeguards outlined in Title II.

2. Sudden abolition of requirements for individuals to furnish Social Security Numbers (Section 203) is potentially dangerous. A revolt against divulging the number could render non-functional many existing systems operated by the State of Ohio. The economic consequences would be great. We would prefer to have Section 203 apply to new systems only and that the Board be given some authority over the use of the Social Security Number.

3. The philosophy of Federal legislation should be to encourage the State to enact their own laws for the protection of privacy, as in S. 2963, rather than having the Federal Government take all responsibility and then delegate it as in Section 103(a)(3). In Ohio, at least, there is strong interest in creating statutory safeguards and we expect some action in the near future.

4. The economic impact of maintaining a "a complete and accurate record . . . of every access to any personal information in a system" (Section 201(a)(9)) should be examined. If you record every access to every record then you must establish what is essentially another "personal information system". Also, recording every access to every record would be vastly more expensive than recording each use of a system.

5. The length of any statement concerning disputed information (Section 201(a)(5)(c)) will have a profound impact on the cost of storage of information in a computerized system, especially if the data is kept on a direct access medium.

6. Information processors and the criminal justice community should be represented on any board. However, the composition of the board should be weighted in favor of the general citizenry.

Finally, I would like to point out that we in the Department of Administrative Services have been active in investigating the problems of privacy and confidentiality and proposing some solutions. Mr. Jerry Hammett, Deputy Director responsible for the Division of Computer Services, is the Chairman of the Committee on Security, Privacy and Confidentiality for the National Association for State Information Systems (NASIS). During the past year this committee has proposed a model State Information Practices Act which can be used by state legislatures as a basis for drafting legislation covering information systems maintained by state and local governments. Mr. Hammett has testified on this bill before an ad hoc subcommittee of the Senate Government Operations Committee and the Judiciary Subcommittee on Constitutional Rights; I am enclosing a copy of his remarks.[1]

I hope you and your committee will find the comments useful in developing legislation. We share your concern over the invasion of privacy. Should you wish further details on our activities or to draw upon our own research and experience, please feel free to call upon us again.

Sincerely,

JOSEPH J. SOMMER, *Director.*

STATE OF PENNSYLVANIA

COMMONWEALTH OF PENNSYLVANIA,
GOVERNOR'S OFFICE,
Harrisburg, August 9, 1974.

DEAR MS. MACNAUGHTON: With this is a statement made by Governor Shapp recently concerning the rights of privacy of citizens in face of a proposed automated total justice information system.

I believe that Governor Shapp's thinking is close to that of Senator Ervin's and I hope that the Senator will have time to note the statement.

With best regard,

Sincerely,

JOHN P. SENSENIG,
Coordinator of Federal Offices.

COMMONWEALTH OF PENNSYLVANIA,
OFFICE OF THE GOVERNOR,
Harrisburg, July 31, 1974.

GOV. MILTON J. SHAPP WRITES ATTORNEY GENERAL CONCERNING THE PHILADELPHIA EXEMPLARY COURT PROJECT

HARRISBURG, July 31.—In a recent letter to Attorney General Israel Packel, Gov. Milton J. Shapp challenged the potential dangers of the proposed Philadelphia Exemplary Court Project which includes as its basic component an automated total justice information system (TJIS).

Shapp said he fully supported the "goal of the model project" which is to reduce crime by providing comprehensive information to criminal agencies in Philadelphia.

"I am deeply concerned, however, about the potential loss of privacy of citizens that this program represents," Shapp further wrote.

He cautioned the Justice Commission to make every effort to insure for Pennsylvania's citizens "all rights of confidentiality and due process."

The Governor emphasized that certain safeguards are mandatory if Pennsylvania is to maintain the rights of its citizens.

When evaluating the proposal, Shapp said it is essential that the Commission seriously consider the guidelines of the Special Committee of Confidentiality of the Philadelphia Regional Planning Council adopted by the Regional Planning Council on June 20, 1974.

The Governor also underscored the importance of each citizen's right to "request and review the information stored in their 'files'."

In conclusion, the Governor added, "I cannot stress too strongly my conviction that any data system in Pennsylvania have guarantees to protect the rights of individual citizens."

[A copy of the Governor's letter is attached.]

---

[1] See testimony on p. 245.

COMMONWEALTH OF PENNSYLVANIA,
OFFICE OF THE GOVERNOR,
Harrisburg, July 25, 1974.

Hon. ISRAEL PACKEL,
Attorney General,
Main Capital Annex,
Harrisburg, Pa.

DEAR GENERAL PACKEL: I understand that at the next meeting of the Governor's Justice Commission on August 5, 1974, the Commission will have before it the federal discretionary application of the Philadelphia Courts for implementation of the Philadelphia Exemplary Court Project, which includes as its basic component implementation of an automated total justice information system (TJIS).

I fully support the goal of this model program to reduce crime and improve our system of criminal justice by providing comprehensive information to criminal justice agencies in Philadelphia.

I am deeply concerned, however, about the potential loss of privacy of citizens that this program represents. The growing number of data banks and the wide variety of information stored for various purposes represent a real threat to the portection of individual privacy. Not only is there great danger that some of the information presently being collected and stored by private agencies might be used for questionable purposes, but individuals often are unaware such information is being collected and they usually have no right to review it to determine its accuracy.

Therefore, I would request that the Governor's Justice Commission not approve this discretionary application unless the members of the Justice Commission are completely satisfied that citizens who may have information about them stored in the proposed system are guaranteed all rights of confidentiality and due process.

Certainly no proposal should be considered without the guidelines developed by the Special Committee on Confidentiality of the Philadelphia Regional Planning Council, and adopted by the Regional Planning Council on June 20, 1974, to the effect that:

1. A Confidentiality Committee established as a standing committee of the Philadelphia Regional Planning Council prepare standards and safeguards on the right of privacy as to the information system included within the project, and that following adoption of those standards and safeguards by the Regional Council that they be binding upon the TJIS and applied prior to that dissemination or restriction of information by the TJIS; and

2. That the applicant (Philadelphia Courts) agree to the creation of a committee of the Philadelphia Board of Judges (perhaps together with a special committee of the Bar Association) to advise the Confidentiality Committee and the Regional Council as to privacy, standards and safeguards to be implemented, and to further advise the Committee and Regional Council as to planned requirements for the distribution of information on the activities of judges; and to select, promulgate and implement appropriate sanctions for violations of the standards established as to confidentiality.

I also urge the Justice Commission to assure that procedures are adopted which guarantee individual citizens the right to request and review the information stored in their "files" to give them a chance to challenge inaccurate or incomplete data.

I would hope the Law Enforcement Assistance Administration in Washington would adopt regulations and guidelines to guarantee the rights of individuals for any data system in the country. But, if they do not, then I believe the Pennsylvania Governor's Justice Commission must see that these safeguards are adopted by the administrators of the program in Philadelphia.

I cannot stress too strongly my conviction that any comprehensive data system in Pennsylvania have guarantees to protect the rights of individual citizens.

Sincerely,

MILTON J. SHAPP,
Governor.

STATE OF SOUTH DAKOTA

OFFICE OF EXECUTIVE MANAGEMENT,
BUREAU OF ADMINISTRATION,
Pierre, S. Dak., July 29, 1974.

Hon. SAM J. ERVIN, Jr.,
U.S. Senator, Senate Office Building,
Washington, D.C.

DEAR SENATOR ERVIN: Your letter of June 25, 1974, regarding S. 3418, requesting a review of that proposed legislation and our opinion on the desirability and practicability of such a law has been referred to me for response.

I have the following observations:

The desirability of such legislation is high. The instances of violation of personal privacy which S. 3418 would hope to correct are numerous. It is my belief that the undetected and/or quietly suffered instances of these incursions are much more numerous than those that have reached public attention.

As to the practicability, it appears to me that there are two main areas of consideration. First is how extensive and expert need the machinery be to administer such a law? Second is how expensive might that administration be? Data processing, although a relative new science, is a highly specialized field and most violations of privacy have occurred because of the layman's inability to relate adequately to the data processing professionals' arguments.

The bill, in and of itself, does not propose any standards that would seem to me to be particularly unwarranted. However, there are two areas in which the state of South Dakota and this administration are suspicious of all legislation. First, is the area of state's prerogatives to determine data processing organization, expenditures, hardware, and software. We would be unalterably opposed to any legislation or regulations resulting from that legislation, which would limit our state's ability to make determinations in those areas. Our state is small, our revenues are limited, and we would be seriously impacted if such a law or regulation would require a dedicated computer for criminal justice information, for one example.

Secondly, the State of South Dakota is opposed to federal legislation which goes beyond stating high minimum safeguards and defining an individual's rights to privacy. We fear that anything more than this would tend to get lost in the maze of various states' deferring data processing structures.

The 1973–74 sessions of the South Dakota legislation passed Senate Concurrent Resolution 2 which calls for a study by the South Dakota Interim Judiciary Committee of this area of concern. That committee is currently considering the establishment of a bill of data processing rights which encompasses all of the principles outlined in S. 3418. At this time that committee's work is devoted to reviewing the scope of the problem and the remedies to it.

In summary, within the parameters that I have outlined above we are in support of S. 3418. Candidly, we feel that perhaps these parameters should be more clearly spelled out.

Sincerely,

GERALD ANDREWS,
Commissioner, Bureau of Administration.

STATE OF UTAH

OFFICE OF THE GOVERNOR,
Salt Lake City, Utah, July 12, 1974.

Senator SAM J. ERVIN, Jr.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR SENATOR ERVIN: Thank you for your letter of June 25, 1974 in regard to S. 3418 establishing a Federal Privacy Board.

The compilation of confidential files on large numbers of citizens detailing all types of activities has become a routine governmental and business function. Regulation of the collection, maintenance, and dissemination of information

from federal, state, local and private data collection systems is needed. The disclosure requirements of this bill will aid the private citizen in obtaining the information which various data banks have collected about him. Merely opening the system to inspection is a step in the direction of preventing abuse in the utilization of confidential data gathered from individual citizens.

The structure of S. 3418, in general, is good. The disclosure requirements providing for publication of the sources, organization and nature of information collected are straightforward and readily understandable. The reporting requirements do not appear to be particularly time consuming nor expensive in terms of materials and manpower so as to create an onerous burden on organizations maintaining the data systems. The structure of the Federal Privacy Board provides it with the needed independence and power to compel disclosure of required information.

I do, however, have two suggestions. First, that the Federal Privacy Board be provided with the means to set up a system whereby it could furnish a citizen, upon request, with the names of the various federal agencies which maintain files on him. This would considerably ease the burden of the citizen in writing to dozens of federal agencies requesting any information they might have concerning him.

Second, the proposed federal guidelines and disclosure requirements should be strictly applied to federal bodies. Yet, the states should be left with as much power as possible to regulate their own agencies and other private organizations located within the state. For this reason perhaps a provision can be inserted into the act exempting those states from federal regulation which pass legislation substantially similar to S. 3418. While the Utah Legislature has not enacted any laws governing the regulation of personal information contained in data banks, such a provision would afford it an opportunity to consider state control of the problem.

I appreciate the opportunity to have any reports or articles on this subject inserted in the record, but have no materials which I wish to submit at this time.

I hope these remarks will aid the Committee and the Senate in their consideration of S. 3418. I support your efforts in the regulation of the standards and management of data banks containing personal information.

Sincerely,

CALVIN L. RAMPTON, *Governor.*

STATE OF VERMONT

STATE OF VERMONT,
EXECUTIVE CHAMBER,
Montpelier, Vt., July 22, 1974.

Hon. SAM J. ERVIN, Jr.,
Chairman, Senate Government Operations Committee,
337 Old Senate Office Building,
Washington, D.C.

DEAR SENATOR ERVIN: Thank you for giving me the opportunity to respond to your bill on individual privacy and confidentiality of information. The rights which it espouses are basic and potentially endangered by the quantum increase in data collection today.

The State of Vermont is also concerned about this problem and I have directed my staff to work with a joint legislative-executive committee during this summer to develop State legislation. Many of the specifics in your bill will presumably be incorporated in the state statute.

I have circulated your letter and S. 3418 among the various executive departments in order to get comments and suggestions from those who work most closely with information, both as users and as data processing professionals. Support for the principles espoused in the bill and for most of the specific provisions was strong. However, a number of particulars might, in our opinion, either unduly hamper legitimate government operations or subvert the basic purposes of the bill with respect to personal liberty. The following suggestions are offered for your consideration.

1. The whole concept of a privacy board to administer an area so vast as both public and private information gathering is of doubtful value. First, the duties and responsibilities of the board under the bill are so demanding that it will

inevitably become deluged by the sheer mass of paperwork. The solution to this problem will most probably be a still larger organization until, finally, ossification takes place and the board would be unable to act at all. Secondly, the record of regulatory agencies in protecting the rights of the public has been less than outstanding. The suspicion exists, in our State at least, that such a board will sooner or later evolve a "pro information" philosophy which will by definition be "anti privacy". Far better are the results of either legislative or judicial action operating with tightly written, unambiguous statutes. Proper use of existing remedies, both administrative and judicial, can be both effective and timely. In place of the board I suggest a three-fold approach. One, well structured legislation with clearly defined standards for all organizations in the area of data collection and use. Two, the requirement that *all* data systems be open to public scrutiny with regard to policies, procedures, and types of data collected. I suspect that the public airing of the internal workings of a challenged system in a court of law or before a Congressional committee will prove sufficient deterrent to misuse in many cases. Thirdly, the powers to hold hearings, publish the data base directory, and conduct research could easily be delegated to an existing federal agency (perhaps the Office of Management and Budget) with no significant increase in cost.

2. The exemptions to the regulations proposed by your bill are of some concern. Title II, Section 202 (1) exempts from all controls information maintained by a Federal agency where the head of that agency "determines that the release of the information would seriously damage national defense". If our experiences of the past two years have any message, it ought to be that national security and national defense can and will hide a multitude of sins. The true significance of the data to national defense should not be a matter for the agency head concerned to decide—that determination should reside in the courts. Title III, Section 301 (6) appears to exempt private non-profit organizations from the provisions of the act. Since universities and hospitals, among others, occasionally prove themselves less than prudent in the collection and use of data, all information systems should be subject to the full requirements unless that system—not that class of organization—is exempted.

3. A major exception to the rules governing access to and dissemination of personal information is incorporated in the phrase "regular access authority" (Title II, Section 201(d)(2)). Implicit in this concept is the assumption that certain agencies other than the one collecting the data have an inherent right of access to files without complying with the stringent rules for dissemination set forth in the act. It is our contention that all agencies should demonstrate compelling public interest before being granted access to personal information.

4. Information professionals, particularly those in automatic data processing, are most concerned about the effects certain administrative requirements in the bill would have on the cost and effectiveness of data processing systems. Taken in the aggregate, they might as much as double the cost of data processing to states and localities as well as to the federal government. In the interests of efficacy as well as cost-effectiveness, these should be altered.

a. Section 201(a)–(9) "maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority". It is this requirement of the bill which will cause the highest expense for each organization maintaining an information system. It will cause a quantum jump in the software, hardware, personnel, and costs of each information system affected. It may drive some organizations providing necessary and responsible service to society totally out of business. Perhaps such a penalty could be introduced if an organization continually violates the spirit and intent of the access controls, but initially it will generate immense amounts of additional data of questionable value.

b. Section 201(d)–(5). Two concerns are involved here. The first is the entry and maintenance of a dispute file, and the subsequent dissemination of disputes. The maintenance of a "dispute file" should not prove to be unduly burdensome by itself. The wording of item (d), however, might prove both useless and time consuming. Attaching pages of disputes to a report containing many names will probably prove wasteful. What might be of help is noting that an individual's record in disputed and requiring that any action taken on this subject's data must be preceded by reading and taking into account the subject's dispute.

The second is item (f) of the same subsection. In order to fulfill the requirements of this item, an organization will have to keep records of each and every

access; therefore, we have the same reservations as expressed under (a)–(9).

c. Section 201(b)–(2). "No Federal agency shall request an individual to voluntarily disclose personal information unless such a request is specifically authorized by laws" . . . . .

It would be asking a great deal of the Congress to anticipate every legitimate question a Federal agency might need to ask an individual. It would be wiser and more in the spirit of freedom, to specify *inappropriate* questions in legislation. As rewritten this paragraph could read, "No Federal agency shall request an individual to disclose personal information prohibited by law".

Hopefully, these suggested changes will increase the already considerable protection for the individual included in your legislation, while at the same time, making necessary and proper data collection feasible. Certainly the need for protection has become obvious over the past few years. The citizens of Vermont appreciate your efforts in this regard. If I or my administration can be of any further assistance, please feel free to call on us.

Sincerely,

THOMAS P. SALMON.

STATE OF VIRGINIA

OFFICE OF THE ATTORNEY GENERAL,
Richmond, Va., August 26, 1974.

Hon. SAM J. ERVIN, JR.,
Member, U.S. Senate,
Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: This is in reply to your letter of June 25, 1974, in which you requested my comments as to S. 3418 and further inquired as to what action is being taken by the Commonwealth of Virginia in the area of privacy, confidentiality, and security of information systems. I share your concern as to the potential for abuse of the right of privacy which is inherent in information systems, both governmental and private. Such systems are proliferating at an alarming rate, and I am pleased that you have given me the opportunity to comment on pending federal legislation in this area and the action that we have taken in this Commonwealth.

Overall, I am impressed by S. 3418, and wish to commend you and your staff on the draftsmanship of this legislation. I was particularly pleased that the proposed Federal Privacy Board is authorized by § 103(a)(3) to delegate its authority over information systems within a state to such state during such period of time as the Board remains satisfied that the state authority is enforcing the provisions of the Act. It would, however, be my suggestion that it should be mandatory that the Federal Privacy Board delegate its authority to a similar state board which is managing and regulating information systems within the state in a satisfactory fashion under federal legislation or similar state legislation. I am of the opinion that a state board could more efficiently supervise and regulate systems within the state than a federal board.

Section 201(a)(9) of the Bill requires any federal agency, state or local government, or any other organization, which by definition includes private enterprise, maintaining an information system that includes personal information to ". . . maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system. . . ." I am advised by persons having technical expertise in data processing that enforcement of this requirement would create an almost impossible burden for most information systems and that the end result would be a data bank of access records which would be as large or larger than the information system being controlled. Every print-out of information stored in a computer would be an access to information about each and every person identified on the print-out. Thus, there would have to be an access record for each person named in the print-out. Every time a clerk of a large corporation goes to a manual file containing personal information, he or she will be required to record the access. Perhaps, the word "access" could be defined by the Act to include only the dissemination of information to persons outside of the system generating or maintaining the information. It is my opinion that such a definition would make the Act more enforceable from a practical standpoint.

With regard to § 202(2) of the Act, which exempts from its coverage criminal investigatory files compiled by federal, state, or local law enforcement organizations, I would suggest that the exception to the exemption be deleted. In many cases during the course of an ongoing investigation, it would be dangerous or inappropriate to commence criminal prosecution for offenses which might be revealed. For example, in the investigation of criminal activity involving a number of suspects, evidence might be produced at the outset of the investigation which would be sufficient to commence criminal prosecution of some persons, but not all those under investigation; however, it would be inappropriate, and possibly dangerous, to commence prosecution of these persons until the conclusion of the investigation which might consume many months. Yet, the exception would seem to apply the provisions of the Act to information sufficient for prosecution, gathered in the early stages of the investigation, when such information has been maintained for a period longer than is normally necessary to commence prosecution. Thus, persons implicated in the early stages of an investigation might, under the provisions of the Act, be able to legitimately demand access to information about themselves after a period of time longer than "necessary to commence criminal prosecution" against them had passed. This, of course, is a most undesirable result.

As to your question concerning action being taken to regulate information systems in the Commonwealth of Virginia, I am pleased to report that, pursuant to two resolutions passed at the 1974 Session of the General Assembly, intensive study of such information systems in the Commonwealth is being conducted with the objective of presenting legislation regulating information systems to the next Session of the General Assembly. I am enclosing copies of these resolutions for your reference.

Senate Joint Resolution No. 10 created a Commission on Computer Privacy and Security to consider, among other things, the possibility of establishing a Privacy and Security Council for the Commonwealth. At a recent hearing, this Commission heard testimony from representatives of all State agencies maintaining personal information systems. The members of the Commission expressed particular concern that State agencies compile and maintain only such information as is necessary to carry out their statutory functions, that they insure the confidentiality of such information, and that the security of the systems be maintained. At future hearings, this Commission plans to hear from representatives of organizations maintaining personal information systems in the private sector.

In another area, Senate Joint Resolution No. 63 created the Virginia Comprehensive Criminal Justice Information System Task Force to study the exchange, collection, storage, security, privacy, and use of information in the Virginia criminal justice system. As a member of this Task Force, I am hopeful that legislation will be recommended which will place Virginia in a position of leadership among the states in the regulation of criminal justice information systems. It is our objective to recommend legislation which will protect the individual right of privacy, while at the same time recognizing the legitimate interests of law enforcement.

I trust that the information contained in this letter will be helpful in formulating legislation designed to afford appropriate safeguards for individual privacy, and to insure the confidentiality of data stored in information systems as well as the security of such systems.

With kindest regards, I remain,

Sincerely yours,

ANDREW P. MILLER, *Attorney General.*

Enclosures.

LD2725

SENATE JOINT RESOLUTION NO. 63

Offered February 15, 1974

Creating the Virginia Comprehensive Criminal Justice Information System Study Commission.

Patrons—Messrs. Walker, Aldhizer and Warren

Referred to the Committee on Rules

Whereas, a rapid increase in recent years in the volume of crime and of offenders has placed great stress upon the complex structure of the criminal justice system; and

Whereas, recent developments in the area of computer-aided information systems can provide law enforcement and criminal justice agencies with a greatly needed and highly advanced tool in the collection, storage, analysis, exchange and dissemination of information so vital to the continued effective operation and management of the entire criminal justice system; and

Whereas, such computer-aided information systems have the potential for jeopardizing the privacy of individuals; and

Whereas, information stored in such computer-aided systems by law enforcement and criminal justice agencies must remain secure from improper and unauthorized access; and

Whereas, the development of such a comprehensive Criminal Justice Information System requires detailed study in order to adequately address the issues of: the identity of information to be collected and maintained in the systems; the manner and means of its collection and storage; the methods of coordination as between various components of the criminal justice system; the methods of maintaining, analyzing and disseminating such information; the physical location of equipment used to operate the system; the funding of the system; and the security and privacy of the information therein; now, therefore, be it

Resolved by the Senate, the House of Delegates concurring, That there is hereby created the Virginia Comprehensive Criminal Justice Information System Study Commission. The Commission shall be composed of twenty-four members; two members from the

Senate of Virginia appointed by the Committee on Privileges and Elections; four members of the House of Delegates appointed by the Speaker thereof; two members appointed by the Chief Justice of the Supreme Court of Virginia, one representing circuit courts and one representing district courts; the following appointments by the Governor: one sheriff representing the Virginia State Sheriffs' Association from among names submitted by the Association; one representative of the Virginia Association of Chiefs of Police from among names submitted by the Association; the Superintendent of the Department of State Police or his designees; one Commonwealth's Attorney representing a political subdivision with a population of less than twenty-five thousand people; one Commonwealth's Attorney representing a political subdivision with a population more than one hundred thousand people; one attorney with substantial criminal defense experience; the Attorney General or his designee; the Director of the Department of Corrections or his designee; one member of the Probation and Parole Board; one representative of the Virginia Municipal League from among names submitted by the League; one representative of the Virginia Association of Counties from among names submitted by the Association; one member of the Virginia State Crime Commission; one member of the Council on Criminal Justice; one director of a planning district commission; and two persons appointed from the public at large. The Governor shall designate the Chairman of the Commission.

The Commission shall make a full and complete study of all matters relating to the exchange, collection, storage, security, privacy, and use of information in the Virginia criminal justice system, as hereinbefore set forth, and shall make recommendations as to the development and implementation of an expanded and integrated system for the collection, storage and exchange of law enforcement and criminal justice information.

The Division of Justice and Crime Prevention shall provide such assistance as shall be requested by the Commission in the conduct of its study and the preparation of its reports. Other agencies of the State shall cooperate with the Commission when requested.

The Commission may hold such hearings as it deems advisable and shall conclude its study and submit its final report and recom-

37-583 O - 74 - pt. 2 - 40

mendations to the Governor and the General Assembly not later than November one, nineteen hundred seventy-four.

Official Use by Clerks

Agreed to By The Senate	Agreed to By The House of Delegates
with / without amendment	with / without amendment
Date:	Date: .....
.....	.....
Clerk of the Senate	Clerk of the House of Delegates

LD0515

SENATE JOINT RESOLUTION NO. 10

Offered January 22, 1974

Creating a Commission on Computer Privacy and Security.

Patrons—Messrs. Babalas, Michael, Parkerson, Aldhizer, Gray, F. T., Campbell, Brault, Moody, Buchanan, Burruss, Hopkins, Smith, Anderson, DuVal, Andrews, Goode, Townsend, Thornton, Marye, Bendheim and Canada

---

Referred to the Committee on Rules

Whereas, the computer is taking an ever-increasing role in our society; and

Whereas, while these instruments are necessary and important in the business, industrial, and governmental growth of the country, if unchecked, they may cause grave inroads in the privacy of the individual; and

Whereas, a study committee of the federal Department of Health, Education and Welfare has made a study of the problems inherent in the untrammelled use of the computer, and has called upon Congress for legislation to "protect us from the protectors", and calls for the creation of a code of fair information practices for all automated data systems, whether run by governmental agencies or private organizations, and to provide criminal penalties for violations thereof; and

Whereas, other states have created Privacy and Security Councils, and it appears that a study should be made as to the feasibility of establishing such a Council in the Commonwealth; now, therefore, be it

Resolved by the Senate of Virginia, the House of Delegates concurring, That a Commission on Computer Privacy and Security is hereby created. The Commission shall be composed of eleven members, five to be appointed from the membership of the Senate by the Committee on Privileges and Elections, and six to be appointed from the membership of the House of Delegates by the Speaker thereof.

The Commission shall study all aspects of the problems involving personal privacy and liberty in the use of computers, with the

view toward establishing a Privacy and Security Council in the Commonwealth of Virginia. The Commission shall study the experience of other states in the establishment of such a council.

In order to carry out the work of the Commission, there is hereby appropriated from the contingent fund of the General Assembly the sum of twenty-five thousand dollars.

The Commission shall complete its study and report to the General Assembly no later than November one, nineteen hundred seventy-four.

Official Use by Clerks

Agreed to By The Senate	Agreed to By The House of Delegates
with / without amendment	with / without amendment
Date:	Date: .....
.....	.....
Clerk of the Senate	Clerk of the House of Delegates

STATE OF WASHINGTON

OFFICE OF THE GOVERNOR,
Olympia, Wash., August 9, 1974.

Hon. SAM J. ERVIN, JR.,
Chairman,
U.S. Senate Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: I was most pleased to receive copies of Senate Bill 3418 and the Congressional Record excerpts pertaining thereto, as I have become increasingly more concerned with the individual's right to privacy and its protection in light of recent developments throughout the country.

This is an area that we have attempted to address on the state level as well, and we are currently in the midst of legislative hearings on various bills that would seek to protect privacy in regard to telephone communications, credit records, and criminal justice records. After reviewing your bill, I find that I am in agreement with the bulk of it, and would suggest only one major amendment which I believe is needed. Although I believe it is necessary and proper for the federal government to enter into the field of privacy preservation, I would hope that any such bill would not, in effect, preempt the states from adopting differing or more stringent regulations of the various aspects of the privacy area. I believe that this could be accomplished with an amendment that would clearly state that it is the intent of Congress not to preempt the field, and that the states may adopt more stringent regulations. With this sort of amendment, I would wholeheartedly support your efforts to enact this bill, and would be pleased to aid you in whatever way that I can to achieve its passage.

Sincerely,

DANIEL J. EVANS, *Governor.*

WASHINGTON STATE SENATE,
JUDICIARY COMMITTEE,
FORTY-THIRD LEGISLATURE,
Olympia, Wash., June 28, 1974.

MS. MARCIA MACNAUGHTON,
Senate Committee on Government Operations,
Senate Office Building,
Washington, D.C.

DEAR MS. MACNAUGHTON: Thank you for your assistance during our telephone conversation of June 28, regarding privacy legislation. Pursuant to your request, I am enclosing two (2) copies each of the following pieces of legislation:

1. House Bill 1475, relating to release of computer data bank information;
2. Senate Bill 2144, relating to electronic surveillance of private communication—please note that present Washington law makes obtaining a "tap" very difficult;
3. Senate Bill 3094, controlling the use of criminal arrest records;
4. Senate Bill 3095, enacting a state Fair Credit Reporting Act;
5. A proposed draft of another bill on electronic surveillance;
6. A proposed draft of legislation on personality testing.

As the 43rd Washington State Legislature has adjourned, these bills will not become law. However, they are the vehicle for a public hearing scheduled on July 13 on the entire area of privacy. It is also likely that they will be the basis for new legislation in January, 1975. As you will note from reading the bills, they are far-reaching in their scope and will no doubt be subject to modification prior to passage.

The committee is presently preparing reports on several of the bills and when they are ready I will forward you a copy of each one. I hope this gives you some idea of what is going on here in Washington State. Please keep in touch, especially begining in January, so that we may keep you current on developments here.

Sincerely,

BERNARD RYAN,
Research Analyst,
Senate Judiciary Committee.

HOUSE BILL NO. 1475

State of Washington
43rd Legislature
3rd Extraordinary Session

by Representatives Goltz, Perry and Blair

Read first time January 22, 1974, and referred to Committee on Judiciary.

AN ACT Relating to the right of privacy; and adding a new chapter to Title 9 RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Section 1. It is the purpose of this chapter to protect the individual's right to privacy by providing safeguards against the improper disclosure of facts and information about the individual through computer accessible files.

NEW SECTION. Sec. 2. As used in this chapter:

(1) "Administrative purposes" when used in connection with automated personal data systems means using such a system for the purpose of affecting the subject individuals directly as individuals such as for making determinations relating to their qualifications, character, rights, opportunities, or benefits.

(2) "Automated personal data system" means a personal data system that is stored, in whole or in part, in computer-accessible files.

(3) "Computer accessible" means recorded on magnetic tape, magnetic disk, magnetic drum, punched card, or optically scannable paper or film.

(4) "Organization" means any profit or nonprofit corporation, partnership, proprietorship, or other organization including the state of Montana and its various local subdivisions and their various boards, agencies, commissions and bureaus.

(5) "Penalty" means any fine, loss of rights, loss of privileges, or loss of employment.

(6) "Personal data" means all data that (a) describes anything about an individual, such as identifying characteristics,

measurements, test scores, (b) evidences things done by or to an individual, such as records of financial transactions, medical treatment, or other services, and (c) affords a clear basis for inferring personal characteristics or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution.

(7) "Personal data system" means a collection of records kept by one or more organizations containing personal data that can be associated with identifiable individuals whether kept for administrative or statistical reporting and research purposes.

(8) "Political meeting" means any meeting at which candidates for political office are chosen or a principal purpose of which is to permit candidates in a primary election or in a general election to address the public and/or to answer questions from the public.

(9) "Private facts and information" means any facts or information about a person that such person is justified in a reasonable expectation they will not be disclosed or used for some other purpose without his consent.

(10) "Private thoughts, sentiments, emotions, sensations, religious beliefs, philosophical beliefs and political beliefs" are thoughts, sentiments, emotions, sensations, religious beliefs, philosophical beliefs, and political beliefs that the holder has a reasonable expectation will not be disclosed.

(11) "Public notice" means, for an agency of the state of Washington such publication that is required for notice of proposed regulations promulgated by that agency under the administrative procedure act, chapter 34.04 RCW, and for other organizations publication in a newspaper of general circulation in the area in which the organization operates. In any event, copies of such notice must be readily available from the organization upon request.

(12) "Standard universal identifier" means a systematically assigned label that attempts to distinguish an individual from all

others in a way which makes such label unique, permanent, ubiquitous, indispensable, brief, and reliable for all individuals and readily available for anyone who needs it.

(13) "Statistical reporting or research purposes" when used in connection with automated personal data systems means using such a system for the purpose of statistical reporting or research only and not to affect any individual directly.

(14) "Surveillance" means the continuous surreptitious observation of any particular individual or group of individuals or members of a single organization without their knowledge and consent for a period of more than one hour on any one occasion or for more than thirty minutes on two or more occasions within any thirty day period. It shall also include the maintenance by any governmental unit, agency, employee, or agent thereof, of any file of information about a person or group of persons gathered primarily and substantially without that person's or group's participation or knowledge, the gathering and maintenance of which information is not otherwise authorized by law. Each entry of information in any such file shall be deemed to be one "act of surveillance" as that term is used in this chapter.

(15) "Private organization charged with dispensing a governmental benefit" is an organization that dispenses a thing of value to the public or some segment thereof under contract or agreement with a governmental unit or agency thereof. For this purpose, obtaining a license shall not be considered such a contract or agreement.

NEW SECTION. Sec. 3. (1) It shall be unlawful for any person to compel disclosure by force, penalty, or imprisonment or threat of force, penalty or imprisonment, from an individual, his private thoughts, sentiments, emotions, sensations, religious beliefs, philosophical beliefs, and political beliefs, except in proper legal proceedings where such individual has himself made such items the subject of litigation.

(2) It shall be unlawful for any governmental unit or agency thereof or any private organization charged with dispensing a governmental benefit to require from any individual as a condition for the receipt of any position or employment or the enjoyment of any right or other benefit an oath, affirmation, or test that probes into such individual's religious, political, or philosophical beliefs.

(3) It shall be unlawful for any governmental unit or agency thereof or any private organization charged with dispensing a governmental benefit to require without express legislative authorization (a) a disclosure from any individual as a condition for the receipt of a benefit or the enjoyment of a right of his membership in or affiliation with or attendance at meetings of any association, group, or other organization the disclosure of which may reasonably amount to a disclosure in part and against his will of his religious, philosophical, or political beliefs, and (b) a disclosure from any association, group, or organization of the names and addresses of any one or more of its members provided said privacy is necessary for the undertaking and continuation of the lawful activities of said association, group, or organization of the names and addresses of any one or more of its members provided said privacy is necessary for the undertaking and continuation of the lawful activities of said association, group, or organization. The determination of whether or not such an individual or association is entitled to claim privacy under this provision shall be made by a judge of a district court in camera in a proper legal proceeding.

NEW SECTION. Sec. 4. It shall be unlawful:

(1) For any person or governmental unit or agency thereof to require as a condition of employment or continued employment that an applicant or employee submit to a polygraphic detection deception test, commonly known as a lie detector test, or to questioning under the effect of thiopental sodium or to any other test or questioning by means of any mechanical device or chemical substance. It shall not be unlawful, however, for an employer to request or suggest a

polygraphic detection deception test for certain specified employees upon the existence of reasonable cause to believe that some one or more of them have committed a criminal offense related to their employment;

(2) For any person or governmental unit or agency thereof to discharge any employee solely because of an alleged or actual opinion that the employee did not tell the truth during a polygraph detection deception test or questioning under the effect of thiopental sodium or any other test or questioning by means of any mechanical device or chemical substance, except where a valid and voluntary stipulation has been executed by the employer and the employee prior to such examination;

(3) For any court in the course of any civil trial, criminal trial or pre-trial proceeding to require, suggest, or request that either the plaintiff or the defendant submit to a polygraphic detection deception test or to questioning under the effect of thiopental sodium or to any other test or questioning by means of any mechanical device or chemical substance.

(4) For any examiner or operator of any polygraph or other mechanical device or chemical test or his assistants or any other person made privy to such information to disclose or use any information acquired during the conduct of such test without the consent of the person examined.

NEW SECTION. Sec. 5. (1) It shall be unlawful for any governmental unit or agency thereof or any private organization charged with dispensing a governmental benefit to require any individual as a condition for employment or the enjoyment of any right or other benefit to take a psychological personality inventory test such as the Minnesota Multiphasic Personality Inventory, the Minnesota Counseling Inventory, and the Edwards Personal Preference Schedule without first having published regulations pursuant to the administrative procedure act, or, if inapplicable, in a manner similar thereto, setting forth the compelling interest that outweighs

this intrusion on an individual's privacy.

(2) Except as set forth in section 6 of this 1974 act, it shall be unlawful for any officer of any executive department or any executive agency of the state of Washington or of any local subdivision or agency thereof, or for any person acting or purporting to act under his authority, to require or request, or to attempt to require or request, any employee of said department, governmental unit, or agency, or any person applying for such employment, to (a) answer any questions designed to elicit from him information concerning (i) his race, religion, or national origin, or the race, religion or national origin of any of his forbears, (ii) his personal relationship with any person connected with him by blood or marriage, (iii) his religious beliefs or practices, (iv) his attitude or conduct with respect to sexual matters, (v) his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household, or (b) make a report concerning any of his activities or undertakings unless such activities or undertakings are related to the performance of his job or to the development of additional qualifications for his job or unless there is reason to believe that he is engaged in outside activities or employment in conflict with his official duties.

NEW SECTION. Sec. 6. Nothing contained in section 5 of this 1974 act shall be construed to prohibit (1) inquiry concerning the citizenship of any such employee or person if his citizenship is a statutory condition of his obtaining or retaining employment, (2) a physician from eliciting such information or authorizing such tests in the diagnosis or treatment of any such employee or person in an individual case basis only where such physician deems such information necessary to enable him to determine whether or not such individual is suffering from mental illness, (3) an officer of such department or agency from advising any such employee of a specific charge of sexual misconduct made against that employee, and affording

him an opportunity to refute the charge, (4) any employee of a taxing authority from obtaining the necessary information to carry out the functions of his job, and (5) with regard to the items contained in subsection (2) (a) (v) of section 5 of this 1974 act only, the requirement of a full disclosure of assets and income by an elected official and the requirement of a full disclosure of any matter which might tend to indicate a conflict of interest in respect to the performance of any of his duties by any other employee or applicant.

NEW SECTION. Sec. 7. The following shall apply with regard to automated personal data systems in order to insure privacy of personal files:

(1) Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an automated personal data system, shall make no transfer of such data to another organization, without the prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an automated personal data system.

(2) Any organization maintaining an automated personal data system shall identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the compliance with these safeguards.

(3) Any organization maintaining an automated personal data system shall take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about the requirements of this section and any rules and procedures promulgated by such organization to assure compliance with them.

(4) No organization shall take any disciplinary or other punitive action against any individual who brings to the attention or appropriate authorities, the press, or any member of the public,

evidence of noncompliance with this section. Any organization maintaining automated personal data systems shall provide a system of penalties for any employee who initiates or otherwise contributes to any such disciplinary action.

(5) Any organization maintaining an automated personal data system shall take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system.

(6) No transfer of individually identifiable personal data to another system may be made without the informed consent of the subject individual, provided a transfer from one system to another within the same organization may be made without such consent if the conditions of the transfer provide substantial assurance that the requirements for security and limitations of access will not be weakened by the transfer.

(7) Any organization maintaining an automated personal data system for administrative purposes shall maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given.

(8) Any organization maintaining an automated personal data system for administrative purposes shall maintain data in the system with such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such data.

(9) Any organization maintaining an automated personal data system that is used in any way for administrative purposes shall eliminate data from computer accessible files when the data are no longer timely.

(10) Any organization maintaining an automated personal data system that is used for statistical reporting and research purposes

shall have the capacity to make fully documented data readily available for independent analysis.

(11) Any organization maintaining an automated personal data system for administrative purposes that publicly disseminates statistical reports or research findings based on personal data drawn from the system, or from administrative systems of other organizations, shall make such data publicly available for independent analysis on reasonable terms, and shall take reasonable precautions to assure that no data made available for independent analysis will be used in a way that might reasonably be expected to prejudice judgments about any individual data subject's character, qualifications, rights, opportunities, or benefits.

(12) Any organization maintaining an automated personal data system shall give public notice of the existence and character of its system once each year. Any organization maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

(a) The name of the system;

(b) The nature and purpose or purposes of the system;

(c) The categories and number of persons on whom data are maintained or are to be maintained;

(d) The categories of data maintained or to be maintained, indicating which categories are stored or are to be stored in computer-accessible files;

(e) The organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

(f) The categories of data sources;

(g) A description of all types of use made or to be made of data, indicating those involving computer accessible files, and

including all classes of users and the organizational relationships among them;

(h) In an automated personal data system used for administrative purposes, the procedures whereby an individual can (i) be informed if he is the subject of data in the system; (ii) gain access to such data; and (iii) contest their accuracy, completeness, pertinence, and the necessity for retaining them;

(i) In an automated personal data system used for statistical reporting and research, the procedures whereby an individual, group, or organization can gain access to data used for this purpose for independent analysis;

(j) In an automated personal data system used for statistical reporting and research, a statement of the system's provisions for data confidentiality and the legal basis for such provisions.

(k) The title, name, and address of the person immediately responsible for the system.

(13) Any organization maintaining an automated personal data system shall inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the organization, of providing or not providing such data.

(14) Any organization maintaining an automated personal data system for administrative purposes shall inform an individual, upon his request, whether he is the subject of data in the system, and, if so make such data fully available to the individual, upon his request, in a form comprehensible to him: PROVIDED, That any information about such individual received from a third person before the effective date of this 1974 act on the condition that such information would remain confidential need not be disclosed in the absence of a court order requiring such disclosure.

(15) Any organization maintaining an automated personal data system shall not allow any use of individually identifiable data that

is not within the stated purposes of the system as reasonably understood by the individual, unless informed consent of the individual has been explicitly obtained.

(16) Any organization maintaining an automated personal data system for administrative purposes shall inform an individual, upon his request, about the uses made of data about him, including the identity of all persons and organizations involved and their relationships with the system.

(17) An organization shall not make data from an automated personal data system available in reponse to a demand for data made by means of compulsory legal process, unless it has first notified the individual to whom the data pertains of the demand and has made the data being sought fully available to such individual.

(18) An organization maintaining an automated personal data system for administrative purposes shall develop and maintain procedures that (a) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; (b) permit data to be corrected or amended when the individual to whom they pertain so requests; and (c) assure, when there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data.

Any organization may obtain a waiver or exemption of any portion or all of any one or more of the requirements of this section from the business and professions administration of the department of motor vehicles pursuant to the procedures promulgated for this purpose by said department upon a showing of a clearly paramount and strongly justified societal interest in such waiver or exemption.

NEW SECTION. Sec. 8. It shall be unlawful for any officer, employee, or agent of an organization maintaining an automated personal data system or any person who has received information from such a system without proper authority or without the informed

consent of the subject individual to disclose any personal data received from such a system that can be identifiable with or traceable to specific individuals except (1) disclosures made in the ordinary course of the business or activity contemplated by the system as set forth in their annual public notice, (2) disclosures made with the informed consent of the subject individual, and (3) by order of or response to a subpoena of a district court. Any person in charge of or privy to information contained in any such system used exclusively for statistical reporting or research may not be compelled to disclose any such data in any criminal or civil proceedings in any court of law of this state. Adequate precautions must be taken to insure that any data released in statistical form by any such system will not reasonably result in the identification of individual data subjects in violation of this provision.

NEW SECTION. Sec. 9. It shall be unlawful for any person to require by means of withholding or threatening to withhold the enjoyment of any right or benefit the disclosure of an individual's social security number issued by the social security administration of the United States or any other label that is functionally similar to a standard universal identifier; provided, however, this provision shall not apply to (1) federal agencies and federal agents acting under lawful federal authority, (2) any person granted specific authority to use such number or label by the legislature, and (3) the department of revenue of when such use is connected with its function of collecting taxes. It shall also be unlawful for any person to use such a number or label for promotional or commercial purposes.

37-583 O - 74 - pt.2 - 41

SENATE BILL NO. 2144

State of Washington
43rd Regular Session

By Senators Durkan, Sandison, Twigg, Gardner, Sellar and Matson (By Municipal Committee Request)

Read first time January 15, 1973, and referred to JUDICIARY COMMITTEE.

AN ACT Relating to private communications between two or more persons; adding new sections to chapter 9.73 RCW; repealing section 1, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.030; repealing section 2, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.040; repealing section 3, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.050; repealing section 4, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.060; repealing section 5, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.070; repealing section 6, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.080; repealing section 1, chapter 48, Laws of 1970 ex. sess. and RCW 9.73.090; repealing section 2, chapter 48, Laws of 1970 ex. sess. and RCW 9.73.100; and providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Section 1. This act shall be known and may be cited as the "Washington State Electronic Surveillance Control Act".

NEW SECTION. Sec. 2. As used in this act:

(1) "Wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by wire, cable or other like connection between the point of origin and the point of reception furnished or operated by a telephone, telegraph or radio company for hire as a communication common carrier;

(2) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

(3) "Intercept" means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device;

(4) "Intercepting device" means any device or apparatus that can be used to intercept a wire or oral communication other than:

(a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a communication common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business, or being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; or

(b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(5) "Person" means any individual, trust, partnership, corporation, association, or any officer or employee of the state of Washington, its agencies, and political subdivisions thereof;

(6) "Law enforcement officer" means any officer of the state of Washington or of a political subdivision thereof who is empowered by law to conduct investigations of, and to make arrests for, any offense enumerated in section 8 of this act;

(7) "Contents", when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication;

(8) "Court of competent jurisdiction" means the superior court;

(9) "Judge" or "court", when referring to a judge or court authorized to receive applications for, and to enter, orders authorizing interceptions of wire or oral communications, means one of the several judges of the superior court to be designated from time to time by order of the supreme court of the state of Washington

to receive application for, and to enter, orders authorizing interceptions of wire and oral communications pursuant to this act;

(10) "Communication common carrier" means any person engaged as a common carrier for hire, in intrastate, interstate, or foreign communication by wire or radio or in intrastate, interstate, or foreign radio transmission of energy, but a person engaged in radio broadcasting shall not, while so engaged, be deemed a common carrier;

(11) "Aggrieved person" means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed.

NEW SECTION. Sec. 3. Except as otherwise specifically provided in this act, any person who:

(1) Wilfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire or oral communication; or

(2) Wilfully discloses or endeavors to disclose to any other person the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the unlawful interception of a wire or oral communication; or

(3) Wilfully uses or endeavors to use the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the unlawful interception of a wire or oral communication;

shall be guilty of a gross misdemeanor. Subsections (2) and (3) of this section shall not apply to the contents of any wire or oral communication, or evidence derived therefrom, that has become common knowledge or public information.

NEW SECTION. Sec. 4. It shall not be unlawful under this act for:

(1) An operator of a switchboard, or an officer, agent or employee of a communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose

or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication. No communication common carrier shall utilize service observing or random monitoring except for mechanical or service quality control checks.

In addition, it shall not be unlawful under this act for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to a law enforcement officer who, pursuant to this act, is authorized to intercept a wire or oral communication;

(2) A person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception; or

(3) Police and fire personnel to record incoming telephone calls to police and fire stations for the purpose of verifying the accuracy of reception of emergency calls. In addition, video and/or sound recordings may be made of arrested persons by police officers responsible for making arrests or holding persons in custody before their first appearance in court. Such video and/or sound recordings shall require strict conformity to the following:

(a) The arrested person shall be informed that such recording is being made and the statement so informing him shall be included in the recording;

(b) The recording shall commence with an indication of the time of the beginning thereof and terminate with an indication of the time thereof;

(c) At the commencement of the recording the arrested person shall be fully informed of his constitutional rights, and such statements informing him shall be included in the recording;

(d) The recordings shall only be used for valid police or court activities;

(4) Video and/or sound recordings obtained by police personnel under the authority of subsection (3) of this section shall be made available for hearing and/or viewing by defense counsel at the request of defense counsel whenever a criminal charge has been filed against the subject of the video and/or sound recordings;

(5) A person not acting under color of law to intercept, disclose, or use a wire or oral communication, where such person is a party to the communication unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this state, or one of the parties to the communication has given express consent prior to such interception, disclosure, or use: PROVIDED, That the consent given for the interception, disclosure, or use of the communication has not been withdrawn prior to publication of such communication.

NEW SECTION. Sec. 5. Except as otherwise specifically provided in section 6 of this act, any person who:

(1) Wilfully possesses an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication;

(2) Wilfully sells an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication;

(3) Wilfully distributes an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication;

(4) Wilfully manufactures or assembles an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication; or

(5) Wilfully places in any newspaper, magazine, handbill, or other publication any advertisement of any intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication or of any

intercepting device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire or oral communication;

shall be guilty of a gross misdemeanor.

NEW SECTION. Sec. 6. It shall not be unlawful under this act for:

(1) A communication common carrier or an officer, agent or employee of, or a person under contract with a communication common carrier, in the usual course of the communication common carrier's business; or

(2) A person under contract with officers, agents, employees, or political subdivisions of the United States or the state of Washington to invent, possess, sell, distribute, manufacture or assemble, or advertise any intercepting device, the design of which may render it primarily useful for the purpose of surreptitious interception, while acting in furtherance of the appropriate activities of the United States, a state, or political subdivision thereof, or a communications common carrier.

NEW SECTION. Sec. 7. Any intercepting device which is invented, manufactured, assembled, possessed, used, sent, or distributed in violation of this act is hereby declared to be a nuisance and may be seized and forfeited to the seizing law enforcement agency.

NEW SECTION. Sec. 8. The Washington state attorney general, any county prosecutors, or persons designated to act for and to perform duties during their absence or disability, may authorize in writing, an ex parte application to a superior court judge designated to receive the same by order of the supreme court of the state of Washington for an order authorizing the interception of a wire or oral communication by the law enforcement officers or law enforcement agency having responsibility for an investigation, when such interception may provide evidence of the commission of the offense of murder, kidnaping, unlawful gambling, robbery, bribery, extortion,

arson, loan sharking, receiving stolen property, the manufacture, possession, or distribution of a controlled substance, or other crimes dangerous to life, limb, or property, or involving threats of violence or injury to life, limb, or property, and punishable by imprisonment for more than one year, or any conspiracy to commit any of the foregoing offenses or any conspiratorial activity of organized crime relative to any offense, or which may provide evidence aiding in the apprehension of the perpetrator of any of the foregoing offenses.

NEW SECTION. Sec. 9. Each application for an order of authorization to intercept a wire or oral communication shall be made in writing upon oath or affirmation and shall state:

(1) The authority of the applicant to make such application;

(2) The identity and qualifications of the law enforcement officers or agency for whom the authority to intercept a wire or oral communication is sought and the identity of whoever authorized the application;

(3) A particular statement of the facts relied upon by the applicant, including:

(a) The identity of the particular person, if known, committing the offense and whose communications are to be intercepted;

(b) The details as to the particular offense that has been, is being, or is about to be committed;

(c) The particular type of communication to be intercepted;

(d) The character and location of the particular wire communication facilities involved or the particular place where the oral communication is to be intercepted;

(e) A statement of the period of time for which the interception is required to be maintained, if the character of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular statement of facts establishing

probable cause to believe that additional communications of the same type will occur thereafter;

(f) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) Where the application is for the renewal or extension of an order, a particular statement of facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results;

(5) A complete statement of the facts concerning all previous applications, known to the individual authorizing and to the individual making the application, made to any court for authorization to intercept a wire or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each application; and

(6) Such additional testimony or documentary evidence in support of the application as the judge may require.

NEW SECTION. Sec. 10. Upon consideration of the facts submitted by the applicant the court may enter an ex parte order, as requested or may modify the order as the circumstances may require, authorizing the interception of a wire or oral communication if the court determines that there is or was probable cause for the belief that:

(1) The person whose communication is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an offense as provided in section 8 of this act;

(2) Particular communications concerning such offense may be obtained through such interception;

(3) Normal investigative procedures with respect to such

offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) The facilities from which, or the place where, the wire or oral communications are to be intercepted, are or have been used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by, such individual; and

(5) The law enforcement officers or agency to be authorized to intercept the wire or oral communication are qualified by training and experience to execute the interception sought.

NEW SECTION. Sec. 11. If the facilities from which a wire communication is to be intercepted are public, no order shall be issued unless the court, in addition to the matters provided in section 10 of this act, determines that there is a special need to intercept wire communications over such facilities.

If the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, or are leased to, listed in the name of, or commonly used by, a licensed physician, an attorney-at-law, or practicing clergyman, or is a place used primarily for habitation by a husband and wife, no order shall be issued unless the court, in addition to the matters provided in section 10 of this act, determines that there is a special need to intercept wire or oral communications over such facilities or in such places. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this act, shall lose its privileged character.

NEW SECTION. Sec. 12. Each order authorizing the interception of any wire or oral communication shall state:

(1) The judge is authorized to issue the order;

(2) The identity of, or a particular description of, the person, if known, whose communications are to be intercepted;

(3) The character and location of the particular communication

facilities as to which, or the particular place of the communication as to which, authority to intercept is granted;

(4) A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates;

(5) The identity of the law enforcement officers or agency to whom the authority to intercept a wire or oral communication is given and the identity of whoever authorized the application; and

(6) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

No order entered under this section shall authorize the interception of any wire or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this act. In no case shall an order entered under this section authorize the interception of wire or oral communications for any period exceeding thirty days. Extensions or renewals of such an order may be granted for periods of not more than thirty days. No extension or renewal shall be granted unless an application for it is made in accordance with this section, and the court makes the findings required by this section and sections 10 and 11 of this act.

An order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the

person whose communications are to be intercepted. Any communication common carrier, landlord, custodian, or person furnishing such facilities or technical assistance shall be compensated therefor by the applicant at the prevailing rates.

Whenever an order authorizing an interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the court may require.

NEW SECTION. Sec. 13. Whenever, upon informal application by an authorized applicant, a judge determines there are grounds upon which an order could be issued pursuant to this act, and that an emergency situation exists with respect to the investigation of conspiratorial activities of organized crime, or related to an offense designated in section 8 of this act, dictating authorization for immediate interception of wire or oral communication before an application for an order could with due diligence be submitted to him and acted upon, the judge may grant verbal approval for such interception without an order, conditioned upon the filing with him, within forty-eight hours thereafter, of an application for an order which, if granted, shall recite the verbal approval and be retroactive to the time of such verbal approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for an order is denied. In the event an application for an order is not made within forty-eight hours, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this act. However, applicants who have not met the requirements of this section are not precluded from submitting applications for future interceptions authorized by sections 10, 11, and 12 of this act: PROVIDED, That the evidence obtained in violation of this section shall not be the basis for determining that probable cause exists under sections 10 and 11 of this act.

In the event no application is made or an application made pursuant to this section is denied, the court shall require the wire, tape or other recording of the intercepted communication to be delivered to, and sealed by, the court and such evidence shall be retained by the court in accordance with section 14 of this act and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person pursuant to section 24 of this act or as otherwise authorized by court order. Failure to effect delivery of any such wire, tape or other recording shall be punishable as contempt by the court directing such delivery. Evidence of verbal authorization to intercept an oral or wire communication shall be a defense to any charge against the law enforcement officer for engaging in unlawful interception.

NEW SECTION. Sec. 14. Any wire or oral communication intercepted in accordance with this act shall, if practicable, be recorded by tape, wire or other comparable method. The recording shall be done in such a way as will protect it from editing or other alteration. Immediately upon the expiration of the order or extensions or renewals thereof, the tapes, wires or other recordings shall be transferred to the judge issuing the order and sealed under his direction. Custody of the tapes, wires or other recordings shall be maintained wherever the court directs. They shall not be destroyed except upon an order of such court and in any event shall be kept for ten years. Duplicate tapes, wires or other recordings may be made for disclosure or use pursuant to subsection (1) of section 17 of this act. The presence of the seal provided by this section, or a satisfactory explanation for its absence, shall be a prerequisite for the disclosure of the contents of any wire or oral communication, or evidence derived therefrom, under subsection (2) of section 17 of this act.

NEW SECTION. Sec. 15. Applications made and orders granted pursuant to this act and supporting papers shall be sealed by the court and shall be held in custody as the court shall direct and

shall not be destroyed except on order of the court and in any event shall be kept for ten years. They may be disclosed only upon a showing of good cause before a court of competent jurisdiction.

Any violation of the provisions of this section may be punished as contempt of the issuing or denying court.

NEW SECTION. Sec. 16. Within a reasonable time but not later than ninety days after the termination of the period of the order or of extensions or renewals thereof, or the date of the denial of an order applied for under section 13 of this act, the issuing or denying judge shall cause to be served on the person named in the order or application, and such other parties to the intercepted communications as the judge may in his discretion determine to be in the interest of justice, an inventory which shall include:

(1) Notice of the entry of the order or the application for an order denied under section 13 of this act;

(2) The date of the entry of the order or the denial of an order applied for under section 13 of this act;

(3) The period of authorized or disapproved interception; and

(4) The fact that during the period wire or oral communications were or were not intercepted.

The court, upon the filing of a motion, may in its discretion make available to such person or his attorney for inspection such portions of the intercepted communications, applications and orders as the court determines to be in the interest of justice. On an ex parte showing of good cause to the court the serving of the inventory required by this section may be postponed.

NEW SECTION. Sec. 17. (1) Any law enforcement officer who, by any means authorized by this act, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may use such contents or evidence or may disclose such contents or evidence to another law enforcement officer to the extent that such disclosure or use is appropriate to the proper performance of the official duties of the officer making or receiving the

disclosure.

(2) Any person who, by any means authorized by this act, has obtained any information concerning any wire or oral communication or evidence derived therefrom intercepted in accordance with the provisions of this act, may disclose the contents of such communication or derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of this or another state or of the United States or before any federal or state grand jury.

(3) The contents of any intercepted wire or oral communication, or evidence derived therefrom, may otherwise be disclosed or used only upon a showing of good cause before a court of competent jurisdiction.

NEW SECTION. Sec. 18. When a law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization, the contents thereof, and evidence derived therefrom may be disclosed or used as provided in subsection (1) of section 17 of this act. Such contents and any evidence derived therefrom may be used under subsection (2) of section 17 of this act when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this act. Such application shall be made as soon as practicable.

NEW SECTION. Sec. 19. Except as specifically authorized pursuant to this act any person who uses or discloses the existence of an order authorizing interception of a wire or oral communication or the contents of, or information concerning, an intercepted wire or oral communication or evidence derived therefrom, is guilty of a misdemeanor.

NEW SECTION. Sec. 20. The contents of any wire or oral communication intercepted in accordance with the provisions of this

act, or evidence derived therefrom, shall not be disclosed in any trial, hearing, or proceeding before any court of this state unless not less than ten days before the trial, hearing, or proceeding the parties to the action have been served with a copy of the order and accompanying application under which the interception was authorized.

The service of inventory, order, and application required by this section may be waived by the court where it finds that the service is not practicable and that the parties will not be prejudiced by the failure to make the service.

NEW SECTION. Sec. 21. Any aggrieved person in any trial, hearing, or proceeding in or before any court or other authority of this state may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that:

(1) The communication was unlawfully intercepted;

(2) The order of authorization is insufficient on its face;

(3) The interception was not made in conformity with the order of authorization.

The motion shall be made at least ten days before the trial, hearing, or proceeding unless there was no opportunity to make the motion or the moving party was not aware of the grounds for the motion. The court, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication, or evidence derived therefrom, as the court determines to be in the interests of justice. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall not be received in evidence in the trial, hearing, or proceeding.

In addition to any other right to appeal, the state shall have the right to appeal from an order granting a motion to suppress if the official to whom the order authorizing the intercept was granted shall certify to the court that the appeal is not taken for purposes

of delay. The appeal shall be taken within the time specified by the rules of court and shall be diligently prosecuted.

NEW SECTION. Sec. 22. Within thirty days after the expiration of an order or an extension or renewal thereof entered under this act or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the administrator for the courts stating that:

(1) An order, extension, or renewal was applied for;

(2) The kind of order applied for;

(3) The order was granted as applied for, was modified, or was denied;

(4) The period of time for which such interceptions are authorized by the order, and the number and duration of any extensions or renewals of the order;

(5) The offense specified in the order, or extension or renewal of an order;

(6) The identity of the person authorizing the application and of the law enforcement officer and agency for whom it was made; and

(7) The character of the facilities from which or the place where the communications were to be intercepted.

NEW SECTION. Sec. 23. In addition to reports required to be made by applicants pursuant to federal law, all judges of the superior court authorized to issue orders pursuant to this act shall make annual reports on the operation of this act to the administrator for the courts. The reports by the judges shall contain (1) the number of applications made; (2) the number of orders issued; (3) the effective periods of such orders; (4) the number and duration of any renewals thereof; (5) the crimes in connection with which the conversations were sought; (6) the names of the applicants; and (7) such other and further particulars as the administrator for the courts may require.

The chief justice of the supreme court shall annually report to the governor and the legislature on such aspects of the operation

37-583 O - 74 - pt. 2 - 42

of this act as he deems appropriate including any recommendations for legislative changes or improvements to effectuate the purposes of this act and to assure and protect individual rights.

NEW SECTION. Sec. 24. Any person whose wire or oral communication is intercepted, disclosed or used in violation of this act shall have a civil cause of action against any person or agency who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, such communication in violation of this act; and shall be entitled to recover from any such person:

(1) Actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation, or one thousand dollars, whichever is higher;

(2) Punitive damages; and

(3) A reasonable attorney's fee and other litigation costs reasonably incurred.

NEW SECTION. Sec. 25. A good faith reliance on a court order authorizing the interception shall constitute a complete defense to a civil or criminal action brought under this act or to administrative proceedings brought against a law enforcement officer.

NEW SECTION. Sec. 26. If any section, subsection or portion or provision of any section or sections of this act or the application thereof by or to any person or circumstances is declared invalid, the remainder of the section or sections or subsection of this act and the application thereof by or to other persons or circumstances shall not be affected thereby.

NEW SECTION. Sec. 27. The following acts or parts of acts are each repealed:

(1) Section 1, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.030;

(2) Section 2, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.040;

(3) Section 3, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.050;

(4) Section 4, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.060;

(5) Section 5, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.070;

(6) Section 6, chapter 93, Laws of 1967 ex. sess. and RCW 9.73.080;

(7) Section 1, chapter 48, Laws of 1970 ex. sess. and RCW 9.73.090; and

(8) Section 2, chapter 48, Laws of 1970 ex. sess. and RCW 9.73.100.

NEW SECTION. Sec. 28. Sections 1 through 26 of this act are hereby added to chapter 9.73 RCW.

SENATE BILL NO. 3094

State of Washington
43rd Legislature
3rd Extraordinary Session

By Senators Mardesich, Woody and Francis

Read first time January 17, 1974, and referred to JUDICIARY COMMITTEE.

AN ACT Relating to criminal record information; amending section 2, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.705; amending section 7, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.730; amending section 9, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.740; adding a new chapter to Title 10 RCW; and prescribing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Section 1. DEFINITIONS. (1) "Law enforcement agency" means any public agency which creates or stores criminal record information.

(2) "Arrest record" means any entry by a law enforcement agency into written record or electronic data banks which identifies a particular person who has been arrested. The term "arrest record" shall include, but shall not be limited to, the following: Photographs made of a person while under arrest, fingerprints taken of a person while under arrest, written offense reports describing the circumstances of an arrest, subjective evaluation by the investigating officer, records indicating the fact that a named person is or has been in jail in connection with pending charges, records indicating that a named person has forfeited bail.

(3) "Conviction record" means a final judgment of conviction of a crime for which a jail term may be assessed, together with any subsequent orders or judgments of a court concerning the sentence, detention, probation, parole, or release of a person convicted of such crime.

(4) "Criminal record information" includes arrest records and conviction records and abstracts thereof as well as records

maintained by any public agency regarding the detention, probation, parole, or release of a named person who has been convicted of a crime for which a jail term may be assessed.

NEW SECTION. Sec. 2. PROHIBITION ON MAINTENANCE AND DISSEMINATION OF CRIMINAL RECORDS. Except as otherwise provided in this chapter, it shall be unlawful for any person or organization to maintain, use, disclose, disseminate, or publish criminal record information.

NEW SECTION. Sec. 3. USE OF CRIMINAL RECORD INFORMATION. (1) Criminal record information may be used for law enforcement purposes.

(2) It shall be unlawful for arrest records to be used for other than law enforcement purposes.

NEW SECTION. Sec. 4. DISSEMINATION OF CRIMINAL RECORD INFORMATION. (1) No arrest record may be disseminated to any federal law enforcement agency or a law enforcement agency of any other state until a final judgment of conviction of a crime is obtained based on the conduct which is the subject of such arrest record.

(2) No arrest record shall be disseminated to any individual, partnership, corporation, or association.

NEW SECTION. Sec. 5. MAINTENANCE OF ARREST RECORDS. In the event that an arrest does not result in a conviction of a crime the arrest record relating to such arrest shall be destroyed by every law enforcement agency having such record within one hundred twenty days after such arrest. If an arrest results in a conviction of a crime which is subsequently reversed by any court, such record shall also be destroyed within sixty days of the time the reversal becomes final.

NEW SECTION. Sec. 6. USE OF CRIMINAL RECORD BY NEWS MEDIA. (1) Except as provided in subsection (2) of this section, information contained in current criminal record information except that which would tend to disclose the identity of the arrestee or convict may be disseminated to, and disclosed by, the news media for the purpose of

informing the public of current events.

(2) Notwithstanding the prohibition of subsection (1) of this section, information contained in current criminal records tending to disclose the identity of the arrestee or convict may be disseminated to, and disclosed by, the news media provided that such dissemination and disclosure may reasonably be expected to aid in the apprehension or conviction of the criminal suspect.

NEW SECTION. Sec. 7. THE EFFECT OF CRIMINAL RECORD INFORMATION ON LICENSING APPLICATIONS. (1) No person, board, commission, bureau, or other entity charged with the responsibility of licensing or otherwise permitting or prohibiting persons from engaging in particular occupations, avocations, professions, or other forms of gainful employment shall deny a license or permission because of an arrest, the record of which has been destroyed pursuant to section 5 of this 1974 amendatory act.

(2) In no event shall any such person, board, commission, bureau or other entity deny such license or permission because of a record of arrest or other conviction unless the facts involved in said arrest or conviction constitute a bona fide occupational disqualification for the type and character of work sought to be performed.

NEW SECTION. Sec. 8. EFFECT OF RECORD DESTRUCTION. (1) Any arrest the record of which has been destroyed as provided in section 5 of this 1974 amendatory act shall be deemed in law not to have occurred, and a person may lawfully deny its occurrence without being guilty of perjury or false swearing under any circumstances.

(2) In any application for employment, license, or other permission to work, or in any appearance as a witness, a person shall not be asked whether or not he has ever been arrested when such arrest has not resulted in a conviction.

NEW SECTION. Sec. 9. PENALTIES AND REMEDIES. Any person with respect to whom criminal record information is being maintained, disseminated, or used in violation of this chapter shall have a cause

of action for writ of mandamus or mandatory injunction against those responsible for such violation and shall be further entitled to recover:

(1) Actual damages, but not less than liquidated damages computed at the rate of five hundred dollars a day for each day of violation, or portion thereof, or one thousand dollars, whichever is higher; and

(2) Punitive damages, but not less than five thousand dollars; and

(3) Reasonable attorney fees and other litigation costs reasonably incurred.

Sec. 10. Section 2, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.705 are each amended to read as follows:

Upon the receipt of identification data from criminal justice agencies within this state, the section shall immediately cause the files to be examined and upon request shall promptly return to the contributor of such data a transcript of the record of previous arrests and dispositions of the persons described in the data submitted.

Upon application, the section shall furnish to criminal justice agencies a transcript of the criminal offender record information available pertaining to any person of whom the section has a record.

For the purposes of RCW 43.43.700 through 43.43.800 the following words and phrases shall have the following meanings:

"Criminal offender record information" includes, and shall be restricted to identifying data and public record information recorded as the result of an arrest or other initiation of criminal proceedings and the consequent proceedings related thereto. "Criminal offender record information" shall not include intelligence, analytical, or investigative reports and files.

"Criminal justice agencies" are those public agencies within or outside the state which perform, as a principal function,

activities directly relating to the apprehension, prosecution, adjudication or rehabilitation of criminal offenders.

Applications for information shall be by a data communications network used exclusively by criminal justice agencies or in writing and information applied for shall be used solely in the due administration of the criminal laws or for the purposes enumerated in RCW 43.43.760 (3).

Any person who, in violation of *this 1972 act, furnishes to any person or other agency information obtained from the section shall be civilly liable, as provided in RCW 72.50.170.

The section may refuse to furnish any information pertaining to the identification or history of any person or persons of whom it has a record, or other information in its files and records, to any applicant if the chief determines that the applicant has previously misused information furnished to such applicant by the section or the chief believes that the applicant will not use the information requested solely for the purpose of due administration of the criminal laws or for the purposes enumerated in RCW 43.43.760 (3). The applicant may appeal such determination and denial of information to the advisory council created in RCW 43.43.785 and the council may direct that the section furnish such information to the applicant.

No information under this section shall be used or made available in violation of sections 1 through 9 of this 1974 amendatory act.

Sec. 11. Section 7, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.730 are each amended to read as follows:

(1) ((When any person, having no prior criminal record, whose fingerprints and/or other identifying data were submitted to and filed at the section, shall be found not guilty of the offense for which the fingerprints and/or other identifying data were sent to the section, or be released without a conviction being obtained, his fingerprints and/or other identifying data and all copies thereof on file at the section shall be destroyed by the section, provided such

~~person requests said destruction after the finding of not guilty or after the releaser))~~ Fingerprints and other identifying data and all copies thereof on file at the section shall be destroyed as prescribed in sections 1 through 9 of this 1974 amendatory act. The section shall, upon destruction of the record pursuant to this section, notify said person of the destruction.

(2) Any individual shall have the right to inspect criminal offender record information on file with the section which refers to him. If an individual believes such information to be inaccurate or incomplete, he may request the section to purge, modify or supplement it and to advise such persons or agencies who have received his record and whom the individual designates to modify it accordingly. Should the section decline to so act, or should the individual believe the section's decision to be otherwise unsatisfactory, the individual may appeal such decision to the superior court in the county in which he is resident, or the county from which the disputed record emanated or Thurston county. The court shall in such case conduct a de novo hearing, and may order such relief as it finds to be just and equitable.

(3) The section may prescribe reasonable hours and a place for inspection, and may impose such additional restrictions, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them: PROVIDED, That the section may charge a reasonable fee for fingerprinting.

Sec. 12. Section 9, chapter 152, Laws of 1972 ex. sess. and RCW 43.43.740 are each amended to read as follows:

Except as provided in RCW 43.43.755 relating to the fingerprinting of juveniles:

(1) It shall be the duty of the sheriff or director of public safety of every county, and the chief of police of every city or town, and of every chief officer of other law enforcement agencies duly operating within this state to furnish within seventy-two hours

from the time of arrest to the section the required sets of fingerprints together with other identifying data as may be prescribed by the chief, of any person lawfully arrested, fingerprinted, and photographed pursuant to RCW 43.43.735.

(2) Law enforcement agencies may, subject to sections 1 through 9 of this 1974 amendatory act, retain and file copies of the fingerprints, photographs, and other identifying data and information obtained pursuant to RCW 43.43.735. Said records shall remain in the possession of the law enforcement agency as part of the identification record and are not returnable to the subjects thereof.

NEW SECTION. Sec. 13. There is added to Title 10 RCW a new chapter to read as set forth in sections 1 through 9 of this 1974 amendatory act.

NEW SECTION. Sec. 14. Section headings as used in this 1974 amendatory act shall constitute no part of the law.

NEW SECTION. Sec. 15. If any provision of this 1974 amendatory act, or its application to any person or circumstance is held invalid, the remainder of the act, or the application of the provision to other persons or circumstances is not affected.

SENATE BILL NO. 3095

State of Washington
43rd Legislature
3rd Extraordinary Session

By Senators Mardesich,
Woody and Francis

Read first time January 17, 1974, and referred to JUDICIARY COMMITTEE.

AN ACT Relating to credit information; adding a new chapter to Title 19 RCW; and providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Section 1. STATEMENT OF PURPOSE. It is the purpose of this chapter to augment the federal Fair Credit Reporting Act and assist in the regulation of the flow of credit information in order to assure that such credit information is accurate and that the consumer's right of privacy is not violated.

NEW SECTION. Sec. 2. DEFINITIONS. For purposes of this chapter:

(1) The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

(2) The term "consumer" means an individual.

(3) The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used on collected in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for:

(a) Credit or insurance to be used primarily for personal, family, or household purposes, or

(b) Employment purposes, or

(c) Other purposes authorized under section 3 of this 1974 act. The term does not include:

(i) Any report containing information solely as to

transactions or experiences between the consumer and the person making the report,

(ii) Any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device, or

(iii) Any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosure to the consumer required under section 12 of this 1974 act.

(4) The term "investigative consumer report" means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on, or with others with whom he is acquainted, or who may have knowledge concerning any such items of information.

(5) The term "consumer reporting agency" means any person which from monetary compensation, on a cooperative nonprofit basis, or otherwise engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumer for the purpose of furnishing consumer reports to third parties. For purposes of this definition the term, third party, shall include and apply to separate agencies of government and subdivisions or other entities thereof.

(6) The term "file" when used in connection with information on a consumer is all of the information on that consumer recorded and retained by a consumer reporting agency, regardless of how the information is stored.

(7) The term "employment purposes" when used in connection with a consumer report means a report used for the purpose of

evaluating a consumer for employment, promotion, reassignment or retention as an employee.

(8) The term "medical information" means information or records obtained with the consent of the individual to whom it relates from licensed physicians or medical practitioners, hospitals, or other medical or medically related facilities.

NEW SECTION. Sec. 3. PERMISSIBLE PURPOSES OF CONSUMER REPORTS. A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(1) In response to the order of a court having jurisdiction to issue such an order.

(2) In accordance with the written instructions of the consumer to whom it relates.

(3) To a person who has a legitimate economic need for the information contained in the file, and who shall identify himself to the consumer reporting agency, certify the purposes for which the information is sought, and further certify that the information will be used for no other purpose. A consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by the prospective user prior to furnishing the user a report. For purposes of this section, a legitimate economic need shall be:

(a) Determining an individual's eligibility for credit;

(b) Determining an individual's eligibility for insurance;

(c) Determining an individual's eligibility for employment, promotion, reassignment, or retention;

(d) Determining an individual's eligiblilty for a license or other benefit granted by governmental instrumentality required by law to consider an applicant's financial responsibility or status.

NEW SECTION. Sec. 4. REPORTING OF OBSOLETE INFORMATION. (1) Except as authorized under subsection (2) of this section, or otherwise subject to any law which provides that such information shall not be provided, or shall be provided for a shorter time than

provided herein, in which case such other law shall apply, no consumer reporting agency may make any consumer report containing any of the following items of information:

(a) Bankruptcies which from the date of an ajudication of the most recent bankruptcy antedate the report by more than seven years,

(b) Suits and judgments which from the date of entry antedate the report by more than six years or until the governing statute of limitations has expired, whichever is the longer period,

(c) Paid tax lands which from the date of payment antedate the report by more than six years,

(d) Accounts placed for collection or charged to profit and loss which antedate the report by more than six years,

(e) Records of arrest, indictment, or conviction of crime which from date of disposition, release, or parole antedate the report by more than six years,

(f) Any other adverse items information which antedate the report by more than six years.

(2) The provisions of subsection (1) of this section are not applicable in the case of any consumer credit report to be used in connection with:

(a) A credit transaction involving or which may reasonably be expected to involve a principal amount of fifty thousand dollars or more,

(b) The underwriting of life insurance involving or which may reasonably be expected to involve a face amount of fifty thousand dollars or more, or

(c) Employment of any individual on annual salary which equals or which may reasonably be expected to equal twenty thousand dollars or more.

NEW SECTION. Sec. 5. DISCLOSURE OF INVESTIGATIVE CONSUMER REPORTS. A person may not procure or cause to be prepared an investigative report on any consumer unless:

(1) That consumer has given a specific dated and separately

signed affirmative written indication of his authorization of such an investigative consumer report after receiving clear and conspicuous written disclosure to him of the nature and scope of such report, or

(2) The report is to be used for employment purposes for which the consumer has not specifically applied.

NEW SECTION. Sec. 6. DISCLOSURES TO CONSUMERS. (1) Every consumer reporting agency shall upon request and proper identification of any consumer clearly and accurately disclose to the consumer:

(a) All information in its files on the consumer at the time of the request,

(b) The sources of the information, and

(c) The recipients of any consumer report on the consumer which it has furnished.

(2) The requirements of subsection (1) of this section respecting the disclosure of sources of information and the recipients of consumer reports do not apply to information received or consumer reports furnished prior to the effective date of this 1974 act, except to the extent that the matter involved is contained in the files of the consumer reporting agency on that date.

NEW SECTION. Sec. 7. CONDITIONS OF DISCLOSURES TO CONSUMERS; TIMES AND NOTICE. (1) A consumer reporting agency shall make disclosures required under section 6 of this 1974 act during normal business hours and on reasonable notice.

(2) The disclosures required under section 6 of this 1974 act shall be made to the consumer:

(a) If he appears in person and furnishes proper identification, the consumer is entitled to personal visual inspection of his file,

(b) By telephone without charge to the consumer if he has made a written request with proper identification for telephone disclosure,

(c) By mail if he has made a written request with proper

identification for mail disclosure, and

(d) By providing a copy of his file if requested at a charge not to exceed actual cost of copying.

(3) Any consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him pursuant to section 6 of this 1974 act. Information furnished by mail must be accompanied by an explanation if furnished in code or trade terminology.

(4) The consumer shall be permitted to be accompanied by one other person of his choosing who shall furnish reasonable identification. A consumer reporting agency may require the consumer to furnish a written statement granting permission to the consumer reporting agency to discuss the consumer's file in such person's presence.

NEW SECTION. Sec. 8. PROCEDURE IN CASE OF DISPUTED ITEM. (1) If any consumer disputes the completeness or accuracy of any item of information contained in his file, he or she may give notice in writing to the consumer reporting agency specifying what items are disputed and in what manner they should be corrected. The consumer reporting agency shall provide forms for such notice and shall assist the consumer in preparing such notice when requested.

(2) Within fifteen days of the receipt of such notice of inaccuracy a consumer reporting agency shall in writing either:

(a) Deny the inaccuracy,

(b) Admit the inaccuracy, or

(c) State that it has not been able to either verify or disprove the disputed information.

(3) If a consumer reporting agency admits the inaccuracy or states that it has been unable to either verify or disprove the disputed information, then the consumer reporting agency shall promptly correct the disputed item of information in the consumer's file in the manner requested in the notice of inaccuracy. The consumer reporting agency shall at the consumer's request inform of

this correction any person who has previously received a report containing the disputed information. The consumer reporting agency shall clearly and conspicuously disclose to the consumer his rights to make such a request. If the consumer reporting agency subsequently determines that the disputed information was accurate and can be verified then it may again include such information in its report.

(4) If the reinvestigation does not resolve the dispute the consumer may file a brief statement setting forth the nature of the dispute. The consumer reporting agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute.

(5) Whenever a statement of a dispute is filed the consumer reporting agency shall in any subsequent similar report containing the information in question clearly note that it is disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.

(6) The consumer reporting agency shall at the consumer's request notify any person who has previously received a report containing the disputed information of the dispute and provide such person either the consumer's statement or a clear and accurate codification or summary thereof.

NEW SECTION. Sec. 9. CHARGES FOR DISCLOSURES. A consumer reporting agency shall make all disclosures pursuant to section 6 of this 1974 act and furnish all consumer reports pursuant to section 8 (3) and (6) of this 1974 act without charge to the consumer if, within thirty days after receipt by such consumer of a notification pursuant to section 12 of this 1974 act or notification from a debt collection agency affiliated with such consumer reporting agency stating that the consumer's credit rating may be or has been adversely affected, the consumer makes a request under sections 6 or 8 (3) of this 1974 act.

Otherwise the consumer reporting agency may impose a

37-583 O - 74 - pt.2 - 43

reasonable charge, not to exceed the actual cost of reproduction, on the consumer:

(1) For making disclosure to such consumer pursuant to section 6 of this 1974 act, the charge for which shall be indicated to the consumer prior to making disclosure; and

(2) For furnishing notifications of disputes to persons designated by the consumer pursuant to section 8 (6) of this 1974 act, the charge for which shall be indicated to the consumer prior to furnishing such notification and not to exceed the actual cost of reproduction of such notification and mailing costs. No charge of any kind may be made for notifying such persons of the correction of information which is found to be inaccurate or unverifiable under section 8 (3) of this 1974 act.

NEW SECTION. Sec. 10. PUBLIC RECORD INFORMATION FOR EMPLOYMENT PURPOSES. A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall:

(1) At the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency together with the name and address of the person to whom such information is being reported; and

(2) Maintain strict procedures designed to insure that the public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is complete and up to date. For purposes of this subsection, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported.

NEW SECTION. Sec. 11. RESTRICTIONS ON INVESTIGATIVE CONSUMER

REPORTS. Whenever a consumer reporting agency prepares an investigative consumer report, no adverse information in the consumer report, other than information which is a matter of public record, may be included in a subsequent consumer report, unless such adverse information has been verified in the process of making such subsequent consumer report or the adverse information was received within the one month period preceding the date the subsequent report is furnished.

NEW SECTION. Sec. 12. REQUIREMENTS ON USERS OF CONSUMER REPORTS--ADVERSE ACTION BASED ON REPORTS OF CONSUMER REPORTING AGENCIES. (1) Whenever any adverse action is taken, either wholly or partly, because of information contained in a consumer report from a consumer reporting agency the user of the consumer report shall:

(a) Disclose in writing to the consumer against whom such adverse action has been taken:

(i) The reason for taking such adverse action, including reference to the particular item or items of information contained in the consumer report,

(ii) The name, street address, and telephone number of the consumer reporting agency making the report, and

(iii) The fact that the consumer is entitled to a copy of his file from the consumer reporting agency at nominal charge, or to inspect his file at the consumer reporting agency free of charge if visited within thirty days of the receipt of the user's notification; and

(b) Furnish a copy of the consumer report if written or a copy of a summary if the consumer report is oral.

(2) Whenever credit or insurance for personal, family, or household purposes or employment involving a consumer, is denied or the charge for such credit or insurance is increased either wholly or partly because of information obtained from a person other than a consumer reporting agency bearing on the consumer's credit worthiness, credit standing, credit capacity, character, general

reputation, personal characteristics, or mode of living, the user of such information shall disclose in writing the adverse action and the nature of the information to the consumer.

NEW SECTION. Sec. 13. PRIVATE REMEDIES. (1) Failure to comply with any of the provisions of this chapter on the part of any consumer reporting agency or user of consumer reports shall constitute an unfair and deceptive trade practice under chapter 19.86 RCW and shall be subject to the provisions of that chapter: PROVIDED, That any person who is injured in his business or property by an act of the consumer reporting agency or user of consumer reports may bring civil action in superior court to enjoin further violations and shall recover:

(a) Actual damages, but not less than liquidated damages computed at the rate of five hunderd dollars for each violation, and

(b) Punitive damages, but not less than five thousand dollars, and

(c) A reasonable attorney's fee and other litigation costs reasonably incurred.

(2) Any consumer reporting agency or user of consumer reports who violates the provisions of this chapter with respect to a particular consumer report may not assert a defensive privilege, absolute or conditional, in any cause of action arising from the dissemination or distribution of the information contained in such report.

NEW SECTION. Sec. 14. SECTION HEADINGS. Sections headings contained in this 1974 act shall constitute no part of the law.

NEW SECTION. Sec. 15. Sections 1 through 13 of this 1974 act shall constitute a new chapter in Title 19 RCW.

PROPOSED DRAFT LEGISLATION ON PERSONALITY TESTING

An Act relating to personality testing; adding new sections to S –0 chapter 9.73 RCW; and prescribing penalties.

Be It Enacted by the Legislature of the State of Washington:

NEW SECTION. Section 1. There is added to chapter 9.73 RCW a new section to read as follows:

It shall be unlawful for any person, corporation, partnership, organization, governmental department, board, agency, official, or other governmental entity, or any other entity to require or request as a condition of employment or as a condition to continued employment that any person or employee submit to any personality test.

"Personality tests" as used in this section means any oral or written test that goes beyond measurement of intelligence, skills, or aptitudes and seeks to measure or to discover emotional states, traits of character, socio-political beliefs or values, sexual adjustment and general propensities.

NEW SECTION. Sec. 2. There is aded to chapter 9.73 RCW a new section to read as follows:

Any person who, directly or by means of any agent, violates the provisions of section 1 of this 1974 act shall be subject to civil action in superior court for damages, to be brought by any person claiming that a violation of this chapter has injured his person or reputation. A person so injured shall recover:

(1) Actual damages, but not less than liquidated damages computed at the rate of five hundred dollars a day for each day of violation, or portion thereof, or one thousand dollars, whichever is higher; and

(2) Punitive damages, but not less than five thousand dollars; and

(3) Reasonable attorney fees and other litigation costs reasonably incurred.

STATE OF WYOMING

OFFICE OF THE ATTORNEY GENERAL,
Cheyenne, Wyo., August 27, 1974.

Hon. SAM ERVIN, Jr.,
Senator, U.S. Senate,
Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: Your request for comments from this office on S. 3418 has been referred to me for answer. You should first know, however, that the State of Wyoming is in the process of establishing a comprehensive Criminal Justice Information System and I have, therefore, taken the liberty of soliciting comments from the Director of that Project, Mr. Edward Coffey, as well as the Advisory Committee on the Office of the Attorney General before responding to your request.

S. 3418 is described as ". . . A bill to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, state and local governments, and other organizations regarding such information, and for other purposes." It appears that this bill seeks to establish a Board to compliment and carry out some of the provisions of your earlier Bill S. 2963 (Criminal Justice Information Control and Protection of Privacy Act of 1974).

While S. 2963 deals solely with Criminal Justice Information Systems, ". . . the purposes of this legislation are to impose certain restrictions upon the type of information which can be collected and disseminated by law enforcement agencies on the Federal, State, and local levels: to place limitations upon the interchange of such information both among such agencies and outside the criminal justice community and otherwise to protect the privacy and reputations of persons about whom the agencies have collected information.", S. 3418 deals with *all* information systems, both public and private. There, therefore, appears to be some duplication which centers around the establishment of separate Boards to oversee each of the separate Acts. While the number and composition of Board members is different, the functions are similar. It would seem that the Federal Privacy Board (S. 3418) could handle, and even supercede, the functions of the Federal Information Systems Board (S. 2963). Apparently the intent is to separate the Criminal Justice Information System

functions from other systems; this may have value but also it may cause problems, i.e., which Board takes precedence?

Based upon your request, I will proceed to go through the provisions of S. 3418 and list the comments which I think to be most important on the separate items.

1. *Creation of the Federal Privacy Board.* I am inclined to agree with Clarence Meyer, Attorney General of Nebraska in his prepared statement of March 5, 1974 to the United States Senate Judiciary Subcommittee on Constitutional Right. I think creation of this Board will free law enforcement officers from the necessity of making policy decisions which they are not equipped to make, in that Federal standards will determine *who* is allowed to get *what* information. As General Meyer notes, law enforcement really does not care if anyone outside of law enforcement ever sees a criminal history, the pressure for release of information comes from without the system.

I would personally welcome a definitive statement on which agencies (non-law enforcement) have the right-and need-to-know prerequisites. Along these lines, however, I also feel that S. 3633 (Government Data Bank Right to Privacy Act) would strike a balance between the need for this determination and what should be the State's right to provide input for this determination. Of the two, S. 3418 and S. 3633, and from a Criminal Justice standpoint, S. 3633 would seem to provide more user participation while still providing the same security and privacy protections to those individuals whose files are contained in the data bank.

Again, my only reservation is in the area of the relationship between the Federal Privacy Board and the Federal Information Systems Board, specifically, whether or not there will be a duplication of effort and which one would take precedence.

2. *Collection of Information from the individual to greatest extent possible.* This requirement does not lend itself to a Criminal Justice application as well as it would in some other type of system. Criminal Justice files, for the most part, come from public documents with very little input from the subject himself. Most of the data maintained is recorded historical information on arrests and dispositions and the subject may not always be willing to provide such information. I would recommend that law enforcement be exempted from this requirement as it is not applicable. Much of the motivation for this legislation, I believe, comes from the "bleeding hearts" who are seemingly much more concerned with the civil rights of criminals than with effective law enforcement. This is not to say that criminals do not have civil rights and that law enforcement should know no bounds, but simply to say that somewhere there should be a balance struck which will be for the long-range benefit of society as a whole. The inclusion of the requirements that information come from the individual subject within the scope of a *Criminal* Information System would effectively kill the System.

3. *Releasing information only to agencies with security and privacy requirements and limitations.* My only comment here would be to emphasize the position taken by Project SEARCH that the responsibility for maintaining security and privacy of information rests with the receiving agency. In the same way that the State agency must assure the Federal system of our ability to control information received by the State from it and our resultant responsibility from having the information, so, too, should we have an agreement between the State and the county and local agencies information is forwarded to. It should be and must be the responsibility of the agency ultimately receiving the information to adequately establish and meet security and privacy considerations. A breach on their part would result in an action against the local agency and not the State agency supplying the information. In this respect, we would generally agree with your requirements and limitations on privacy and security.

4. *Transfer of information beyond jurisdiction of the United States.* Such transfer would occur most likely in the area of organized crime and would effect resulting intelligence information such as LEIU information transfers. I feel this requirement impedes the information flow and could effectively destroy the functions of LEIU.

5. *Maintaining a list of persons with regular access.* This provision will create an unnecessary bookkeeping effort on the part of all law enforcement. With the advent of switching hardware which allows direct access from the field to a data base in one state by a terminal in another state, the number of potential users is greatly increased. To maintain a list of all individuals in every agency which has the capability of accessing our files would be a monumental task. Even with a small turnover in every agency in the United States, it would require a huge

additional staff to keep track of "who is allowed access today." I believe the same effect could be had by programming our computer to accept inquiries from law enforcement terminals only, maintaining a record of which terminal accessed information, and requiring the individual agencies to worry about maintaining lists of their own terminal operators.

6. *Individual's right to inspect.* This provision, of course, should be an absolute necessity in any information system where data flows relatively unrestricted between people (see No. 8 below). It would, however, limit the effectiveness of intelligence systems such as LEIU if they are not exempted. You have introduced legislation (S. 2963), which prohibits computerized intelligence files, and if that bill passes, this will be a moot subject. If that portion of the bill is deleted, however, intelligence files must be exempted from examination. If this is not done, intelligence systems will become worthless; subject individuals would know that law enforcement has recognized them; persons would not readily supply information knowing that the subject has the right to know who supplied the information; and subject individuals would know specifically which agencies were interested in them. If LEIU is any example of an organization maintaining intelligence files, and I believe it is, such systems are superconscious of an individual's right to security and privacy, and disclosure of information to unauthorized persons is virtually impossible. We believe that the approach LEIU has taken is valid, and Wyoming plans to follow that example closely.

7. *Right to inspect by mail.* It seems that this provision would relax some of the safeguards that the bill itself is trying to impose. I would suggest that if the individual desires to examine his file, and he does not live within commuting distances to the record repository, that he be required to go to a local law enforcement agency and be fingerprinted and that the request for examination be issued through that agency accompanied by the fingerprint card for comparison purposes and then the information being sent to the individual. The right to inspect by mail without this security requirement defeats the entire concept of privacy and security, since anyone could make a written request for confidential information on not only himself but others.

8. *Notification of file maintained on an individual.* I have already expressed my opinion on the need of this type of provision for other than intelligence files. The introductions to various Bills, are peppered with stories of how an arrest, followed by a warning and dismissal, has come back years later to haunt the individual. We need not go so far from home. The Division of Criminal Identification has records sent in by law enforcement agencies within the State, which record a minor arrest and dismissal and yet carry an FBI number. A nineteen-year-old who is picked up and printed for disturbing the peace, for example, and who is given a warning and released would probably believe that this is the end of his difficulties, he may be very wrong. His fingerprints may have been sent to the FBI and the Division of Criminal Investigation for the State of Wyoming. Years later, in applying for employment, he may reply that he has never been arrested. A check through the FBI or the Division of Criminal Identification will prove him wrong.

Although the requirement to inform individuals of a file being maintained on them will increase the agency's workload, I feel that it is well worth it in preventing such situations as that described above.

9. *"Investingatory files"—definition—exempted from the provisions of this Bill are "Investigatory files".* At the present time, some phrases are used interchangeably but refer to entirely different entities and agencies. I would like to see this phrase defined specifically.

Basically, this office is in favor of the concept of privacy and security as it applies not only to the Criminal Justice Information System, but other public and private systems as well. The above comments are intended to be constructive so as to request that Congress strike a balance between the rights of the citizen and the rights and needs of law enforcement to have access to information. I would like to thank you for your letter, and I do hope that you and your Committee will recognize the very definite needs of law enforcement in this area in a time when crime is on the rise and not in decline.

Sincerely yours,

FRED C. REED,
Deputy Attorney General—Criminal Division.
EDWARD J. COFFEY,
Criminal Justice Analyst Division of Criminal Investigation.

LETTERS AND COMMUNICATIONS

L. S. AYRES AND CO.,
Indianapolis, Ind., July 17, 1974.

Hon. BIRCH E. BAYH, Jr.,
U.S. Senate,
Russell Building,
Washington, D.C.

DEAR BIRCH: Thank you for your July 3 letter in which you ask for a statement on how the elimination of social security numbers from our credit application has worked for L. S. Ayres and Company. We appreciate the opportunity to provide such a statement and offer the following information.

We requested the social security number for many, many years because we did not feel we could live without this information if we were to properly identify our customers. It has been our experience that individuals may change their names, use variations of their names, change their addresses and marital status, but they seldom, if ever, change their social security numbers. It is a reliable form of identification.

The social security number was used by our Credit Department as an aid to identifying customers that had identical names at the credit bureau. It was important from the standpoint that many times the address that we had on our new application was more current than the one at the credit bureau. Therefore, the social security number was helpful in assuring that we obtained a correct credit bureau report on our customer. The social security number was also used as an aid in identification when attempting to locate a customer's new address or as an aid to verify the identity of a customer attempting to purchase merchandise without his credit card and very little identification on his person.

Our company has a sincere appreciation and respect for each individual's right to privacy; and, accordingly, this is one of the factors we consider when designing our procedures. In 1971, you and Senator Ervin issued public statements against the abuse and overuse of the social security number. These statements prompted me to check our procedures, as I also felt that the social security number was being overworked as a form of identity and possibly could lead toward the establishment of a central data bank of information on each and every individual. In March 1971, we investigated our need for the social security number on our applications and determined that it was not absolutely necessary to have this information to properly process and service a charge account. We found that the number of times that we actually needed the social security number to identify an individual was minimal. We decided to delete the social security number from our credit application.

We have not used the social security number for three years, and the problems resulting from this change have been virtually zero. Once in a great while, we may select an incorrect credit bureau report on an individual because of similar names and some confusion relative to the addresses, but generally, the error is discovered before the customer is inconvenienced.

In summary, the elimination of the social security number from our credit application has not adversely affected our ability to properly service our customers, while on the other hand, we feel that in some small way, we have been helpful in reducing the abuse of the social security number and helping our customers protect their right to privacy.

Cordially,

DANIEL F. EVANS.

788 DALBEY DR.,
Las Vegas, N. Mex., June 25, 1974.

Sen. CHARLES PERCY,
U.S. Senate.

DEAR SENATOR: I am enclosing an article which appeared in the Santa Fe, New Mexican June 17, 1974. Like many many Americans I completely endorse your sentiments.

I am also enclosing a xerox copy of a notice I received two days after applying for insurance from State Farm. To protect companies both large and small certain documented evidence is necessary to carry on their business, as it relates to their customers or clients.

I consider and have so notified State Farm (Phoenix Regional Office. And head office in Bloomington Indiana) that I consider question—of my neighbors etc. concerning my character, reputation personal characteristics etc. a complete and unnecessary invasion of my privacy.

Senator, I have absolutely nothing to hide. My statements on my application were completely truthful. In Detroit I had living next door to me in an upper middle class neighborhood a reputed small time Mafia hoodlum. Here in Las Vegas according to an open letter which received wide circulation across the street from me lives one of the top dope pushers in the Las Vegas High School Area. I am sure you have read about "Smack City". Senator would you care to have people like this provide information about you?

Credit reports are a necessary evil in our way of life. *BUT* I feel that when a credit report is requested a report should automatically be submitted to him as well as the company. He should have the right to sue both the company requesting the information and the Agency providing it if it is false. A company should be required by law to notify a customer that a report will be requested in his case before not after accepting his application. When the notice is received after the application a cancellation could be construed as an admission of false statements on the application. This is an untenable situation.

Sorry the letter is so long but as one voter, regardless of this issue's outcome I feel we need more people in Congress who are willing to look ahead and not backward.

Very Sincerely yours,

ROBERT J. ISBISTER.

STATE FARM INSURANCE COMPANIES,
AUTOMOBILE DIVISION.

ROBERT J. ISBISTER,
788 Dalbey Dr., Las Vegas, N. Mex.

INFORMATION REGARDING THE FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act, enacted into law by Congress in 1971, serves to protect consumers against the circulation of inaccurate or obsolete information by a Consumer Reporting Agency. The Act requires that, whenever an insurance company requests an Investigative Consumer Report, the consumer must be notified.

A report has been requested in your case. A Consumer Reporting Agency in completing an investigative Consumer Report including information on an individual's character, general reputation, personal characteristics or mode of living may personally interview neighbors, friends, associates of the consumer or others with whom he is acquainted, or who may have knowledge concerning any such items of information.

The consumer investigated may request in writing, within a reasonable period of time after receiving notice of the investigation, additional information relative to the nature and scope of the investigation.

I have cancelled this request for insurance and taken it out with another company.

Senator, to many Americans this issue is far more important than Watergate. One is constructive the other destructive.

R. ISBISTER.

BETHESDA, MD., *June 19, 1974.*

Sen. CHARLES H. PERCY,
Dirksen Senate Office Building,
Washington, D.C.

DEAR SENATOR PERCY: From the media I have learned that you are conducting an inquiry into "Snooping" both by the government and private source.

This news is indeed welcome! I hope that your inquiry will also include the availability of bank records as will examples such as the enclosed.

I bring to your attention, as an example, a News Week "Subscriber Survey," a copy of which and my reply are enclosed. Unfortunately many gulible people will fall for this type of "Come on."

As you are looking into the matter I will not send a copy of the correspondence to the A.C.L.U.

Should you wish to examine the original "Survey" form I will gladly make it available.

Sincerely yours,

T. H. E. NESBITT.

BETHESDA, MD., *May 30, 1974.*

Mr. ROBERT RIORDAN,
Circulation Director, Newsweek,
The Newsweek Building, Livingston, N.J.

DEAR MR. RIORDAN: Please be advised that I sent Newsweek a check for $22.00 on May 1, 1974. I am advised by my bank that it was cleared on May 9th.

I regretted both actions very much, following receipt of your undated form renewal notice on or about May 23rd., for the following reasons:

1. The question asked under group #3 of the "Newsweek Subscriber Survey" is entirely personal and none of your damn business.

2. Although you state in the introduction of the "Newsweek Subscriber Survey" that "Your answer will, of course, be confidential", the survey portion contains the number 419 3807 769 which is also on my "active subscriber card"—a business machine data card. It is obvious that any information given in the survey will be fed into the "active subscriber file card" which is not marked confidential nor referred to as such. The card thus becomes part of a data bank which can be used indiscriminately.

3. In my opinion this is a thinly veiled, if not blatant and crude attempt to compile lists of individuals and their income category which I consider to be an invasion of privacy.

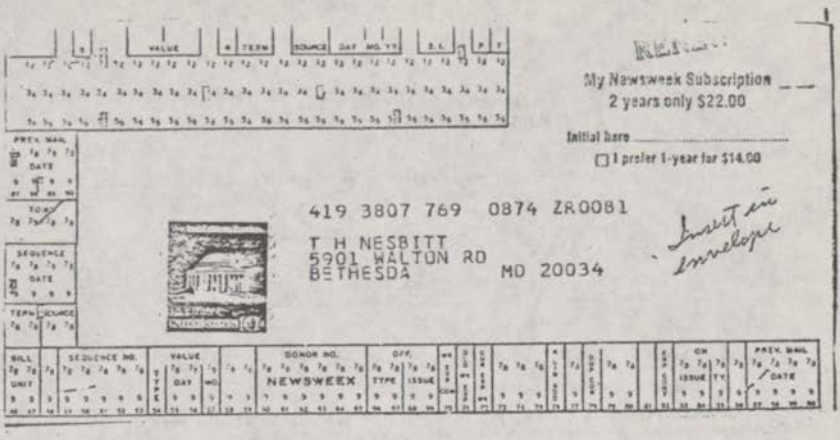
For the above reasons I request that you terminate my subscription and refund the $22.00 (for a two-year subscription) less cost of issues received prior to receipt of this letter.

Yours very truly,

T. H. E. NESBITT.

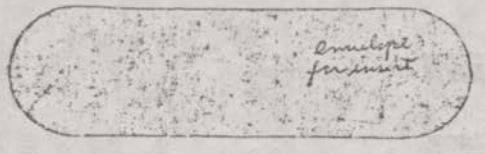
P.S. I may send copies of this letter and your "Survey" to the American Civil Liberties Union and to the appropriate body of the U.S. Congress if your reply is not satisfactory.

Enc. Xerox copy of "Newsweek Subscriber Survey".


My Newsweek Subscription
2 years only $22.00
Initial here
I prefer 1-year for $14.00
419 3807 769 0874 ZR0081
T H NESBITT
5901 WALTON RD
BETHESDA MD 20034
Insert in envelope
NEWSWEEK

IMPORTANT:

Your subscriber file card is enclosed.
PLEASE RETURN IT TODAY!



Dear Subscriber:

Your Newsweek subscription expires soon!

To speed through your renewal -- so you'll not miss a single week of important news -- I've enclosed your active subscriber file card. Please initial and return it at once.

Modern business and tabulating machines are marvels of efficiency, but the punched cards which control them must pass through many departments, and days are required to prepare them. The enclosed card contains all the information we need to continue your subscription uninterrupted.

A special reply envelope is provided to speed handling your card. Please do sign it and use the stamp to return it to us today.

Thank you,

Robert E. Riordan

Robert E. Riordan
Circulation Director

RER/DOE

P.S. And if you haven't already done so, won't you take a moment to fill out our subscriber survey. Without your participation, it can't be a real success. It will help some worthy organizations as well. Thanks.

NEWSWEEK SUBSCRIBER SURVEY

The following questions can be answered quickly and easily, with a check or a word or two.

Please use the envelope provided for your convenience in returning the questionnaire to us.

Answers will, of course, be kept confidential.

149 3807 769

1. What is your business, industry or profession?

A ☐ Agriculture/Forestry
B ☐ Communications/Publishing/Advertising
C ☐ Construction/Mining
D ☐ Education
E ☐ Finance or Banking
F ☐ Government
G ☐ Insurance or Real Estate
H ☐ Manufacturing
I ☐ Professional (MD, Lawyer, etc.)
J ☐ Services to Business
K ☐ Transportation or Public Utilities
L ☐ Travel/Entertainment
M ☐ Wholesale or Retail Trade
N ☐ Other (please specify)

_____

2. What is your title or position? Please check the most appropriate box.

A ☐ Owner, Partner, Director
B ☐ Company President
C ☐ Other Company Officer (Vice-Pres., Treasurer, etc.)
D ☐ Department Head E ☐ Manager
F ☐ Supervisor
G ☐ Other administrative position not mentioned above
H ☐ Scientist or Engineer I ☐ Sales-Equipment
J ☐ Technical Specialist
K ☐ Sales-Merchandise
L ☐ Clerical M ☐ Teacher
N ☐ Foreman, Skilled Craftsman, Laborer
O ☐ Housewife P ☐ Student Q ☐ Retired
R ☐ Military (Rank: _____)
S ☐ Other (please specify) _____

(continued on reverse side)

R.R. No. 1, SMITHSHIRE, ILL., *June 19, 1974.*

Sen. CHARLES PERCY.

DEAR SIR: As I have seen in the papers, you are fighting the invasion of privacy of the citizens of this nation. I thought I would send you this portion of advertisement my Step-mother and I received. It will be enclosed in this letter.

On April 9th 1974, Mother and I bought a new car. After reading this ad material enclosed you will know the make, year, and type. Also my occupation.

This ad arrived about the 17th of June, so you see how little privacy anyone has.

I rather imagine by now even the government has this information in a computer bank. Maybe also the Russians and God alone knows who else.

Now all this information gathering costs money, and I know that a lot of tax funds are being spent this way.

Senator, I know that you used to be a top-notch machinist with Bell & Howell. And I'm sure you didn't appreciate every move you made known, as it seem's to be the case to-day. I hope you will fight this privacy thing, to as a successful conclusion as you did your job with Bell & Howell.

While I'm writing this, I might as well go into other areas.

First of all Welfare,

Since minimum wages, we have knowledge of one case where the man will not work for more than the min. wage and just so many hours so that he can collect food stamps etc. since min. wage went to $2 he has cut off one days work. Much to his employer's dissatisfaction, this same man has a welfare worker haul his wife 11 miles to the laundry mat. This worker gets $2 per hour for this. Welfare even purchased him a sewing machine for his wife & it is said she doesn't even know how to sew. This man is in his 30's.

Another case is a man 47 yrs. old. He owns 14 acres of ground, upon which he lives. His wife is on A.D.C. & has 4 children, (these are her children). He's paid house rent for the above members of his family, then he has 3 children by a previous marrage & he is paid rent for himself & one son. Now, his oldest girl was in Texas & married, she became pregnant and he went to Texas & brought her here for welfare to take care of. More than likely he is collecting rent for her off welfare. He also went back to Texas to try and get her husband to come here, as he was in trouble in Texas something about stealing guns.

He was working for a contractor 7 yrs. ago and claims an injury to his back. Make's him unable to work. But he tears down old building and sells the lumber, also cuts and hauls steel, old cars, machinery etc. In fact, I had him helping me for a few days at $3.50 per hr. There was 2 week's which we couldn't work here and when he came back he claimed he had made a thousand dollar in those two weeks. Now does that sound like a man who couldn't work? Besides this the welfare has paid hospital bills for him of $10,000 or more. From what I can find out they really haven't found to much wrong.

Also, during these 2 weeks which he claimed he made this thousand dollars the welfare bought him a new elect. range & some other appliance. Plus lineolum floor covering.

These are two cases of which I personally know, just in this locale, so just imagine how enormous this must be over the whole nation.

This I do know, this kind of Welfare, Mim. Wage Control etc. makes it very rough for small farmer's & Business to hire help. We just don't have that kind of Incomes. And also people can make more on Welfare than they can working, and no taxes to pay. So in my opinion welfare is cutting the nation's throat. I also feel the Whole situation of Welfare is a vote getting scheme.

Another thing before you can control inflation the Wages of the working man will have to have a max. limit. I've worked out all my life except the last 7 yrs. starting when I was 14 yrs. old & I've advocated this to Paul Douglas when I was working by the Hour & he was on the finance committee.

Welfare is cutting the am't. of Income tax Payer's, making a heavier tax Burden on fewer & fewer People, The Government is spending more & more, in all Ways including trying to buy friendship & Peace. Slowly they are killing the goose that lays the golden egg, then What?

If you read this, I Thank you for your time.

You also have my permission to use this Ad. if it Will Help you make Your Point in your fight.

I remain,

Yours respectfully

JOHN I. ICENOGLE.

FREE INSPECTION CARD — 30-DAY FREE TRIAL

RESERVED FOR THE ICENOGLE FAMILY ONLY

DO NOT WRITE IN THESE SPACES

AUTOMOBILE:
MAKE Ford
YEAR 1974

AIR FLO™ TAILORING DATA:
AUTO MAVERICK
FRONT 0274-4-F
REAR 0274-4-R

CUSTOMER RECORD:
OCCUPATION A-1

M.F.
VALIDATED

FREE! Just for trying the seat covers. No purchase required, you receive FREE TO KEEP: Matching interior accessories including a tailored set of Door Kick Panel Covers, a pair of Visor Covers, and a handy, all-vinyl Litter Bag ... PLUS, a pair of His and Hers Travel Bags AND a Surprise Bonus Free Gift.

437672504

MR. JOHN I. ICENOGLE
RURAL RT. 1
SMITHSHIRE, IL. 61478

9911-5919011 11001-7459 437672-1111C

If address is wrong, please write in new address below old address.

5-010081-000

Detach before Mailing

Affix your pattern stamps to the backside of the card above!

Dear Mr. Icenogle,

0274-4 ← THE NUMBER IN THE BOX AT THE LEFT IS YOUR number ... the Air Flo Pattern Series Number for your new 1974 Maverick 2 Door Sedan.

WHAT DOES IT MEAN TO THE ICENOGLE FAMILY?

Just this! It means there is a way to protect that beautiful new cloth or vinyl upholstery and at the same time make it even more beautiful and more comfortable than it is now.

INSTALL A SET OF TRANSPARENT, CUSTOM TAILORED
1974 MAVERICK AIR-FLO SEAT COVERS

We've measured the upholstery of a 1974 Ford exactly like yours and added it to the one thousand, nine hundred and fifty different custom Air Flo patterns we keep on hand. (We don't have "universal" or "one-size-fits-all" covers like most automotive stores and catalog houses.) The number on the left represents your pattern series, so when you affix your pattern stamp and verify the information on the reverse side of the card above, we know exactly what kind of upholstery you have. Then we can send you a tailored set of Air Flo covers made for your car -- just like they were fitted in a custom trim shop!

And with a set of Air Flo covers protecting your upholstery, you never again have to worry about stains, rips, spots, burn holes, tears ... or, about losing that fresh, natural beauty your Ford upholstery has now.

Because if anything does happen -- if someone drops a cigarette ash or sits down with a sharp object in his pocket or whatever -- the damage isn't permanent. You spoil the seat cover instead of the seat. And we'll replace the worn or damaged Air Flo section -- regardless of what happened, how long you own your car or how many times you need replacements -- for just $1.98 per section.

That's right! Air Flo protects your upholstery ... without hiding it one bit.

WINDOW-CLEAR AIR FLO SEAT COVERS ACTUALLY MAKE YOUR WHOLE INTERIOR MORE BEAUTIFUL

They let all the natural beauty of your upholstery show through, then make it come alive with a soft, star-dust

FREE INSPECTION CARD – 30-DAY FREE TRIAL

FINGERHUT CORPORATION: I have affixed the pattern stamps most closely resembling my car's seating arrangement and filled in the information below. Please accept my order for a set of Air Flo Seat Covers tailored for my car on a 30-Day Free Trial. I understand that if I am dissatisfied with them in any way or for any reason I can return them at the end of 30 days and owe nothing. The FREE GIFTS are mine to keep in either case. (This offer governed by the laws of the State of Minnesota.)

Affix the enclosed pattern stamps most closely resembling car's seating arrangement in the spaces provided below.

Affix Front Seat Stamp Here

Affix Third Seat Stamp Here (3 Seat Station Wagons Only)

Affix Rear Seat Stamp Here

Try a set of Custom-Tailored Air Flo Seat Covers, FREE!

Examples of how to describe car:

YEAR 1974 1973 1972 MAKE Plymouth Ford Chevrolet MODEL Fury Fairlane 500 Bel Air BODY STYLE 2 Door (No. Post) 4 Door 4 Door (Sta. Wag.)

Fill out and return in enclosed envelope.

CAR YEAR _____ MAKE _____

MODEL _____ BODY STYLE _____

Please sign name _____

Phone number _____

OFFICE USE ONLY

Detach before Mailing

glisten. If you think seat covers have to "cover-up" to protect, you'll be amazed when you see how much better your upholstery looks through transparent Air Flo. In fact, a lot of our customers tell us it was the Air Flo look that sold them!

The comfort of Air Flo covers is a big thing too -- both with cloth and vinyl upholstery. Tiny "air pillows" (eight per square inch) let air circulate better for a more comfortable ride.

But I don't expect you to buy a set just because I tell you they'll protect your upholstery, that they're beautiful and comfortable ... or, just because a lot of other people have bought them. And, even though the enclosed sample will give you an idea of what Air Flo vinyl looks like, it can't come close to showing you how beautiful a tailored set will look in your car.

NO-RISK 30-DAY FREE TRIAL

That's the reason I'd like you to try a set of Air Flo covers tailored for your car ... BEFORE YOU BUY. It's the best way I know to show you how really beautiful and rugged Air Flo covers are. Just affix the pattern stamp most closely resembling your car's interior to confirm our records, fill out the Free Inspection Card above and drop it in the mail (postpaid return envelope enclosed). I'll send you a set of Air Flo covers to use as your own for 30 full days -- without obligation. If after 30 days you're not convinced that Air Flo covers are everything I say, just send them back and we'll forget the whole thing.

FREE!

YOUR FREE GIFTS!

And simply for going to the trouble of trying the Free Trial, I'll send you a pair of His & Hers Travel Bags, a Surprise Bonus Free Gift and a complete ensemble of matching interior accessories, ALL YOURS TO KEEP EVEN IF YOU DECIDE NOT TO KEEP THE SEAT COVERS!

But if you're like 12 million other people and find you don't want to be without a set of Air Flo covers in your car, keep them. You can pay for them in one single payment or in easy monthly payments:

	Total Cash Price	Six Payments @	Single Pymt. & Deferred Pymt. Price
Full set	$24.36 + ship. & handl.	$4.35 EA.	$26.10
Front Only	$14.36 + ship. & handl.	$2.63 EA.	$15.78
3 Seat Wagon ..	$36.49 + ship. & handl.	$6.39 EA.	$38.34

(Add $1 each for center armrests, front and rear)

NO FINANCE CHARGES! NO DOWN PAYMENT REQUIRED!

Let's not talk about buying yet, though ... that's for you to decide after you've had a chance to try Air Flo for 30 days FREE. THE IMPORTANT THING NOW IS TO MAIL YOUR FREE INSPECTION CARD before something happens that could damage your new upholstery permanently!

Sincerely yours,

M. Fingerhut

PRESIDENT

MF:eb

ARTICLES AND PUBLICATIONS

[From the (Philadelphia) Evening Bulletin, June 26, 1974]

CURB THE COMPUTERS—DATAMANIA AND PRIVACY

Americans today face an insidious threat to their privacy, one that is growing steadily, almost unnoticed, in the profusion of government and private data banks.

The so-called datamania with which government and private industry compile records on millions of people has reached a point of complexity and unmanageability that should frighten even the most complacent.

A recent report of the Senate judiciary Committee shows that 858 federal data banks are operated by 54 government agencies. Some of these collect "blacklist" information, such as individual protests in civil disobedience, riots and so on.

Some other figures: The Defense Department has dossiers on approximately 1.6 million persons in its industrial security files; the Justice Department maintains a civil disturbance file with 22,000 names and another with 250,000 names in the organized crime section; the National Highway Safety Bureau, 3,300,000 names; the Secret Service, 69,000 persons considered potentially dangerous, etc., etc.

The report estimates that the total of records in Federal Government files exceeds one billion, at least five for every living American. And after the Government comes the private data banks.

The General Services Administration is now seeking a $100 million data system that could link many of the existing government systems, giving thousands of government employes access to information on millions of people at the drop of a switch. The potential for abuse in such a system is obvious.

Data banks are a permanent feature of modern society. All presumably originate in legitimate and worthwhile purposes, a fact which has tended to obscure the potential threat involved. Most do not permit access by individuals on whom the data is being kept to check for the relevancy, accuracy or timeliness of the information.

While the files remain closed to individuals, the information contained on them is easily and regularly traded between government agencies. An individual's habits, his weaknesses, his strengths, his credit worthiness are recorded, often without his knowledge.

What is needed are stringent controls and safeguards against the abuse by data banks, including the right of access by individuals and the chance to review and correct information. The growing complexity and diversity of collection systems also demand the need for simplified procedures and perhaps could justify a single identifying number, such as Social Security, for each individual. Protection against data theft and electronic tapping are essential.

The era of "Big Brother" is upon us. The task now is to have protective legislation that preserves individual privacy and controls the proliferation of new banks.

[Editorial from the Washington Post, July 19, 1974]

CONTROLLING THE DATA BANKS

Congressional concern about preserving civil liberties has been, over the years, a sometimes thing, so many people will be surprised if the current surge of legislative interest in protecting individual privacy actually produces much legislation. There are growing indications, however, that this year Congress might really follow through on at least one major privacy issue by enacting a measure

to regulate data banks and protect citizens against the improper or undisclosed collection and use of personal information by the government.

The need for controls has been amply documented. After four years of work, Sen. Sam J. Ervin's Subcommittee on Constitutional Rights has just released a landmark study which itemizes 858 federal data banks containing over 1.2 billion records on identifiable individuals. Over 86 per cent of these files are computerized. Various data banks hold information on citizens' employment records, medical problems, driving habits, criminal histories, financial dealings, military service and other sensitive subjects. At least 29 files concentrate on derogatory information. In more than 42 percent of the cases, citizens are not notified that such records about them are being kept. And only 16 per cent of all these data banks have been expressly authorized by law. All this is doubly awesome because the study is incomplete. It does not include the White House "enemies lists" or the records maintained by some agencies which refused to cooperate.

Clearly some basic rules need to be set before the government's penchant for collecting information grows any further out of hand. Last year an HEW advisory committee proposed several fundamental principles: that there should be no files whose existence is undisclosed; that citizens should be able to review and correct almost all records about themselves; that information gathered for one purpose should not be used for another without the subject's consent; and that extensive efforts should be made to protect the security and confidentiality of all files. These principles have been incorporated in the Koch-Goldwater bill in the House and in Senate measures sponsored by Sen. Ervin and several colleagues. On both sides of the Capitol, useful hearings have already been held. The legislative efforts have received a strong assist from Vice President Ford, who pushed the Office of Management and Budget to submit some specific recommendations to the Hill.

For all this progress, however, the hard work is just beginning. Major disagreements have surfaced about the way that basic policies should be applied to governmental files as different as, for instance, the FBI's investigative dossiers and the masses of inactive records in the National Archives. Agencies have already started lobbying for exemptions for national security files, personnel records, census data and other categories. Indeed, some modifications will be required. For example, notifying the subjects of all files would be self-defeating for law enforcement agencies; for the Archives it would be impossible. But Congress should resist the pressures to write such broad, permanent exemptions into a law. The prudent course would be to authorize an oversight board to make exemptions in accord with strict guidelines and with ample opportunity for public comments before any data-collecting is allowed to proceed in secrecy.

Another major issue is how ambitious legislation should be. Some bills would reach not only federal files, but also state, local and private data banks. Ultimately those files should also be subject to controls, since citizens can be hurt just as badly by the misuse of private records as by federal mistakes. Yet Congress may not know enough about the multitude of nonfederal files to deal intelligently with them all at once. The difficulties encountered in trying to regulate credit reporting and limit the traffic in arrest records suggest that a careful, step-by-step approach is best outside the federal domains. By reforming the policies for federal agencies and federal aid recipients, this Congress can set a strong example for the states and give citizens far more assurance that they won't be hurt by information lurking somewhere in a data bank.

[From the New York Times, July 17, 1974]

New Discrepancies Found In Controller's Accounts

FUND TOTALS DIFFER

A second audit of the City Controller's office by an outside public accounting concern has uncovered a discrepancy of more than $30-million between city funds deposited with major banks and the Controller's records of those funds.

The audit, performed by Clarence Raines & Co., deals with the citys' general treasury funds. It is separate from an earlier audit, released Sunday, by S. D. Leidesdorf & Co., which found $5.4-million in negotiable securities unaccounted for. They were supposed to have been in a city vault.

The Raines' audit, which is still in draft form and approaching final form, is based upon a check of the Controller's general ledger as compared with bank

records as of Dec. 31—the last day that Abraham D. Beame now Mayor, served as Controller.

If the bank records, as opposed to the Controller's records, are correct, the city has in excess of $30-million more on deposit than it thought it had. The total or deposit, according to the banks, is about $450-million.

Like the earlier audit, the Rainess one was highly critical of security procedures in the Controller's office—this time from the point of view of lax control over check-signing machines employing automatic signature plates.

But unlike the earlier audit, this one appeared to emphasize heavily the likelihood of "bookkeeping" errors to account for the discrepancy, as opposed to fraud, theft or embezzlement.

Among other developments yesterday were the following:

The Mayor and Controller Harrison J. Goldin announced the establishment of a "task force" under Commissioner of investigation Nicholas Scop- during recent years" in the Controller's records on securities in the vault.

The Mayor, who was reported ill with viral bronchitis and remained at Gracie Mansion, did not respond publicly to the disclosure by Mr. Goldin that an audit conducted by Mr. Beame's office found $3.95-million in discrepancies in the securities count as of Dec. 31, 1971.

Yet another audit—the fourth—that was critical of the City Controller's office came to light. This one was performed by State Controller Arthur Levitt in late 1971 and it called for "improving procedures and internal controls" within the office's division of pensions.

A DIFFERENT PICTURE

Taken as a whole, all of the audits paint a picture of loose accountability, lax security, and financial management with adequate internal controls—all of which conflicts with the image of Mr. Beame, who campaigned for Mayor on a record of administrative and fiscal expertise.

Both of the audits performed by the outside public accounting firms were commissioned by Mr. Goldin on March 25 as a means, he said recently, of ascertaining the "status" of the $10-billion in assets that he "inherited" Jan. 1.

The first audit, by Leidesdorf, caused a feud of press releases between Mr. Goldin and Mr. Beame, with each implying that perhaps the blame for the unaccountable securities—which were deposits by contractors to guarantee performance—occurred during the other's administration.

The Mayor was reported to be angry that the Controller released the report without first attempting to "reconcile" the discrepancy and pin down the possibility of mistaken but accidental entries in the ledgers.

Mr. Beame released a statement pointing out that the physical count of the securities in the vault had been taken on March 31—a date that would include three months of the new Controller's tenure.

However, the second outside audit, the Rainess audit verifying general city treasury funds, was based upon a retrospective check of the records of the Controller and the banks the day before Mr. Goldin assumed office.

The general treasury funds, amounting to approximately $1.5-billion, are simply the sum-total of revenue on hand from all sources, such as taxes, Federal and state aid, and proceeds of bonds and note sale.

DEPOSIT PLAN EXPLAINED

A certain amount is on deposit at any given moment with major banks under what is known as the "pool and satellite" system, an investment method designed to increase interest earnings.

The six "pool" banks are: Bankers Trust, Chase Manhattan, Chemical, First National City, Manufacturers Hanover and the Morgan Guaranty Trust Company.

The discrepancy of more than $30-million was arrived at by studying the records of the "pool" banks with those of the Controller's general ledger.

The bank records are apparently more convincing.

"Anyone reading the audit would have the right to assume that the city does in fact have more cash than it thought it had," commented one city official, who said that his name not be used.

An additional sum of cash on hand close to $30-million, could have been significant during the recent budget negotiations. It might have meant, some political observers noted, that there was no necessity for imposing the auto use tax, which is expected to bring in $22-million or the fee on off-track betting, which is scheduled to bring in $30-million.

PROCEDURES SCORED

Critical of the Controller's bookkeeping system, the Raines' audit highlights what it calls "the absence for many years of bank reconciliation procedures."

The "task force" announced by the Mayor and the Controller to look into the securities will draw upon personnel from the city's Department of Investigation, the Manhattan District Attorney's office, and the Police Department's bond and forgery squad.

Its primary objective is to determine whether the discrepancies were "due to faulty bookkeeping procedures or theft."

Interviewed in his office yesterday as he was about to begin the investigation, Mr. Scoppetta said that he had "an open mind" on the matter, but tended initially to suspect faulty bookkeeping because of the "sheer monumental size" of the securities unaccounted for.

[From the Washington Post, July 6, 1974]

POLICE COMPUTER INFORMATION USE INCREASES

Installed six years ago at a cost of more than $6 million, a high speed crime information computer employed by Washington's metropolitan police is increasingly being used in the pursuit of suspects and stolen goods.

Enthusiasm for the computer system is concentrated in the city, and some suburban officials rarely rely on it, using it only when their own systems fail.

Named WALES, the "Washington Area Law Enforcement Systems," the computerized data bank was designed to provide city and suburban policemen with current information on wanted persons, stolen property, guns, auto registrations, parking violations and traffic warrants.

For example, if a policeman in Prince Georges' County stopped a car from Washington, by giving either the license or registration number to WALES, in seconds the officer could find out to whom the car belonged, whether it was stolen, any outstanding traffic violations and whether the driver was wanted for a crime by local police or the FBI.

The financing of the $270,550 WALES design project began with a $30,000 grant to the city by the now defunct Urban Renewal Administration. Then more than $287,000 in federal law enforcement assistance funds was given to the Council of Governments to get the program underway. Since 1968, the metropolitan police budget has allotted over $1 million a year to finance the WALES system.

WALES involves both police and civilians in compiling information from the courts, the police department's data processing division, the department of motor vehicles, and other city agencies.

The main WALES computer is located in the basement of police headquarters at 300 Indiana Ave. N.W. When the program started it was connected to 50 terminals in the Washington area: located in each city police district substation, the police headquarters of every suburban jurisdiction in the metropolitan area, U.S. Park Police headquarters, the Secret Service, the Armed Forces Police, Dulles International Airport and National Airport.

WALES is also tied to the FBI's central computer system housed in Washington, the National Crime Information Center. The data bank that allows immediate checks on crimes and suspects across the country.

Despite the fanfare that accompanied the debut of WALES as the most sophisticated police computer network in the world, it became the object of criticism from suburban police departments.

At that time, complaints about WALES fell mainly into four categories:

Suburban police departments were reluctant to check vehicle records through WALES, fearing out-of-date information might lead to the arrest of innocent drivers.

Although suburban police stations had WALES computers, suburban policemen had to hand-carry punch cards to Washington police headquarters to give WALES information.

WALES computers had a reputation for long shutdown times, or periods of time when the computer was not working.

Maryland and Virginia got their own computer systems that performed many WALES tasks.

Since 1968 the number of WALES terminals used by law enforcement agencies has increased from 50 to 100 in the metropolitan area. The cause of this increase

has been the ability of WALES to supply police departments with more accurate and detailed information.

When WALES began its operation, it relied entirely on the FBI's NCIC computer for information on missing autos. NCIC, however, did not include impounded or repossessed vehicles in its data banks. Now, not only does WALES keep its own records of missing cars reported in Washington, but also has computer operators working round-the-clock to keep the files on autos as current as possible.

Ralph J. Clement, Head of the WALES branch of the D.C. police, and who has been with the program since it began, notes that WALES is now in operation 98 percent of the time, one of the lowest shut-down times for a computer system in the country.

He projected that over 3 million queries would be made of the WALES computer during this year, a 1,000 percent increase over 1968.

The key to the future of WALES, according to Clement, is the expanded use of the cathode ray tube (CRT). This teletype computer with a television screen not only can put information directly into computer banks, but also enables policemen to fill out on-the-spot warrants for any crime committed in the metropolitan area, from stolen guns to bicycles, for missing persons, or other emergencies.

This is done by typing a code word into the computer, depending on the type of warrant to be issued.

A blank "mask" form then appears on the screen to be filled in by the police officer. After the officer fills out the form, the warrant is transmitted to all WALES terminals.

This is particularly important to Washington and neighboring districts, because not all crimes for which warrants are issued are extraditable. Therefore, they would not be on the NCIC computer, but may still be of mutual interest to the District and the suburbs.

An additional benefit of the cathode ray tube system is that it can be tied to a teletype machine that simultaneously gives a "hard copy" of the information flashed on the WALES–CRT screen for police files.

At present there are 65 cathode ray tube machines in operation, all of which are in the Washington area, two belonging to park police. With the teletype machine that gives the "hard copy," each cathode ray tube system costs up to $4,500 a year.

Another feature of the WALES network is its "real time information system" through which any data is immediately put into the WALES computer.

While Maryland has its own computer system, MILES (Maryland Interagency Law Enforcement System), and Virginia its VCIN computer (Virginia Criminal Information Network), the suburbs have not abandoned WALES. Feelings about the effectiveness of WALES in the suburbs range from enthusiastic to cautious.

Captain Clay Taylor of the Prince George's County police department, which uses the system more than any other suburban jurisdiction said, "I'd hate to have anything happen to it. If anything was done to the WALES system, we'd have a problem in Prince George's County." Prince George's County is planning to get a cathode ray tube system this year.

Similarly, Captain Alvin Fuchsman said the Arlington police department "hopes to expand the use of WALES." Arlington also plans to obtain a CRT–WALES system during 1974.

Lieutenant William Hobday, deputy director of the communications of Montgomery County Police, is less generous with his praise for WALES. He said, "We have no plans to drop the WALES system. Although it is of little use to Montgomery County, WALES serves as an excellent backup to the NCIC computer when our MILES terminal is shut down.

In Fairfax County, where there is a large number of autos from Washington and Maryland, WALES enables the local police to check vehicles from the metropolitan area, a capability that the VCIN system does not have.

Since 1971 new WALES terminals have been installed in Falls Church, headquarters of the Military District of Washington, and in the clerk's office of the Washington Superior Court (this includes a WALES–CRT terminal and hard copy teletype).

[From the Washington Post, Sept. 10, 1974]

LATEST POLICE ITEM: PORTABLE COMPUTER TERMINAL

(By Paul Hodge and Alfred E. Lewis)

With 12 pounds and $2,155.60 worth of guns, walkie-talkies, chemical sprays, tickets, handcuffs, billy clubs and slapjacks, keys, whistles and other equipment dangling from their bodies, Washington policemen are, they say, the most lavishly and weightily adorned policemen in the world.

But there's still one item needed to create the ultimate modern policemen, according to department officials: a digital computer. Weighing two pounds and costing an estimated $500 each, hand-held computer terminals are now being developed for all of the city's 4,900 policemen.

The computers eventually will give each other instantaneous feedback on stolen cars, bicycles and other property, wanted criminals, traffic tickets and anything else a policeman might want to know that can be computerized.

They will also take up what little space remains on each officer's Sam Browne Belt, the heavy leather outer belt only motorcycle policemen used to wear but which now is provided all officers because of the profusion of equipment they must tote around.

However, the current 12-pound burden around the midriff is not something most of today's policemen have to walk far with, since there are only a dozen regular foot patrol beats left in the city and only about 200 of the city's 4,900 policemen are actually on foot on any given day.

The vast majority of officers are motorized on or in 360 motor scooters, 14 motorcycles, 545 scout cars, 25 patrol wagons, three helicopters and seven harbor patrol boats with 120 additional scooters and 50 more scout cars soon to arrive. Two officers also patrol regularly on unmotorized vehicles, bicycles.

While motorizing policemen enabled them to respond to crimes more quickly, the walkie-talkie and the present central police computer have given policemen here a quantum jump on criminals in the past few years. Before the advent of the walkie-talkie, first experimented with here in 1961 but given all officers only three years ago, policemen were out of communication whenever they left their radio scout cars. The walkie-talkie eliminated the need for radios in police vehicles. The computer went into operation here in 1968.

The coming digital computer terminals, which are being developed under a $264,000 federal grant, will both speed each officer's access to central police and FBI computers and will also free busy police radio frequencies for crucial messages.

In order to make use of police computers now, an officer must call headquarters on his walkie-talkie and ask for a check on a car license number or a person's name. This is then fed into the computer and a dispatcher calls the officer back with the information.

With the digital computer terminal "each officer will be able to ask a question and within seconds have the information flashed back on his computer screen," says Insp. Thomas F. Wert, head of the police property division.

"The only problem with the concept at the moment is that the terminals will have only 32 characters available on the screen, which will limit the amount of information an officer can get," Wert said.

Many cities already are experimenting with digital computers in scout cars but they are cumbersome units that cost more than $4,000 each, says Wert, compared to the $500 per unit he expects the hand-held terminals will cost.

When the two-pound digital computer is added to the crime-fighting arsenal around the policeman's waist, he will be carrying 14 pounds of equipment, exclusive of his clothing. Already hanging there are a .38-caliber pistol and holster, a two-pound walkie-talkie, ticket book and leather case, handcuffs and leather case, patrol box key, whistle, aerosal chemical spray and cherrywood baton or billy club.

While Washington policemen may have to carry all this equipment at least they don't have to buy it or worry about replacing it. Most policemen in the United States still have to buy their own guns and uniforms—and if they want luxury items like handcuffs they must purchase them, too.

Washington has what Wert calls the country's most advanced quartermaster system, supplying its officers with everything but shoes, socks, underwear, winter gloves and, for some reason, a police whistle (cost 50 cents).

New York City policy officials were here studying Washington's quartermaster system recently, says Wert, but he doubted that New York's Finest would be willing to give up their annual clothes allowances, "especially since they come each year just before Christmas and many officers use it like a Christmas bonus."

Wert said Washington policemen "are already the best-equipped in the world . . . and with the hand-held digital computer terminal . . . ah."

[Reprinted from Minneapolis Tribune, Oct. 7–12, 1973]

YOUR LIFE: HOW PRIVATE?

(By David Kuhn)

> "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficial. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."
>
> Justice Louis D. Brandeis, Olmstead v. U.S., 1928

MENDHAM, N.J.—Lori Paton is a slim, brown-haired senior at West Morris-Mendham High School in the hilly, wooded countryside of north central New Jersey. She was 16 years old last spring when the FBI decided to investigate her.

She had committed no crime. She had engaged in no subversive activity. She had not applied for a sensitive government job.

She merely had written to a left-wing political group, seeking information to fulfill a class assignment.

Her letter was intended for the Socialist Labor Party, but it was sent to the New York address of the Young Socialist Alliance. Apparently the FBI was monitoring all mail sent to that group, noting names and return addresses.

On March 18 an FBI agent walked into Principal Richard Matthews' office to inquire about Miss Paton.

When Miss Paton was told about the visit "it didn't mean much at first." But as she thought about the implications, "It sort of hit me more," she said. Her decision: "I'd rather fight it now than later, when I might end up on some list."

As a result, Miss Paton, her father and the chairman of the school's social studies department filed a lawsuit in July with the aid of the American Civil Liberties Union (ACLU). They are seeking $65,000 in damages and a court order preventing the FBI from intercepting mail sent by citizens to lawful political organizations.

Is the Lori Paton case an isolated one, signifying only that the FBI is guilty of occasional bad judgment?

Or is it just the tip of an iceberg, signifying that the constitutionally protected right to privacy is too often subject to arbitrary and damaging invasion by the agents of government, usually without the citizen ever knowing it?

There is no objective measurement available of the amount of government surveillance and government dissemination of presumably confidential information that goes on daily or yearly.

What is known, however, is that there have been numerous public disclosures of these kinds of activities in the last few years.

Some of the activities were legal but questionable. Others were patently illegal:

In the late 1960s the Army engaged up to 1,500 plainclothes agents in a massive and apparently uncontrolled program of spying and data collection against civilians engaged in lawful political activities.

The chief subjects were civil rights and antiwar groups. Some targets of the surveillance were inexplicable or bizarre. Army agents in the Twin Cities maintained files on Harry Davis and Louis Ervin, both respected black civic leaders. And in May 1969 no less than four agents were assigned to file spot reports from the "Whip to White," which was nothing more than a college beer bust at White, S.D.

New evidence of more recent Army surveillance of civilians, this time against American citizens in West Germany, has been turned up by an investigator for Sen. Lowell Weicker, R-Conn.

The targets of spying and infiltration included a McGovern for President group operating a voter registration effort last fall among Americans in Berlin.

In addition to the burglary and wiretapping of Democratic headquarters and the burglary of a California psychiatrist's office by White House employees acting in the name of national security, the Watergate investigation also uncovered the Tom Charles Huston plan for expanded government surveillance of citizens.

Some of the proposed activities were "clearly illegal," Huston, a White House staff man, had cautioned, but President Nixon approved the plan anyway in 1970, only to rescind it five days later because J. Edgar Hoover, then head of the FBI, wouldn't go along with it.

The plan included FBI burglaries, illegal interceptions of mail, monitoring of overseas telephone and telegraph communications, and intensified electronic surveillance against individuals and groups "who pose a major threat to the internal security."

Huston resigned from the White House in 1971 and is an Indianapolis attorney. He is closing out a term as a member of the Census Bureau's Advisory Committee on Privacy and Confidentiality.

Government agents surveyed the banking records of persons who financially supported unpopular but legal political causes.

Several studies—including the latest one by an advisory committee to the Department of Health, Education and Welfare—have called for safeguards and restraints on computerized data banks used by local, state and federal agencies.

The concerns of a growing number of legislators, legal scholars and private citizens were summed up recently by Sen. Sam Ervin, D-N.C., whose constitutional rights subcommittee was holding hearings on privacy problems long before Watergate occurred.

"Congress, and the American people in general," he said, "are only now becoming aware of the multitude of ways in which our right to privacy—our right to be let alone—is being ever circumscribed by the collection of information about almost every aspect of our lives."

The activities of private agencies, such as credit bureaus, have been recognized as potential or actual invaders of privacy, too.

But government is better equipped to do it, unless restrained. It has much of the information already—census data, tax records, military records, criminal records, photos of driver's license holders, files on welfare recipients—although it would be a costly and technically difficult task to put it together.

Other information may be obtained through exercise of the police power. This includes bank records, mailed matter and oral conversations.

Moreover, as Justice Brandeis warned 45 years ago in his dissent to a 5–4 decision permitting wiretaps, few invasions of privacy and confidentiality arise from an evil intent.

The Army surveillance program, for instance, apparently began with a desire for some advance notice of civil disturbances in which troops might be called in.

"All of these things—you've got to emphasize this—come in under some plausibly beneficial purpose," said Douglass Lea, director of the ACLU's Project on Privacy and Data Collection that was established last spring to disseminate information and give visibility to privacy issues. "People take these mandates and push them to their logical extremes and turn them into threats," Lea said.

The right to privacy is rooted in the English common law. Although "privacy" isn't mentioned in the U.S. Constitution, the Supreme Court and most legal scholars have interpreted the Bill of Rights as a privacy shield.

Frequently or occasionally cited are the First Amendment guarantee of free speech, free association and the right to remain silent; the Third Amendment's protection of the individuals' living space; the Fourth Amendment freedom from unreasonable searches and seizures; the Fifth Amendment protection against self-incrimination; the Ninth Amendment's guarantee that rights not enumerated elsewhere are also to be enjoyed by citizens, and the Fourteenth Amendment's due-process clause.

There is, however, no comprehensive and consistent body of privacy law on the books of the nation or the states. As Arthur R. Miller, a law professor and author of a much-quoted book, "Assault on Privacy," has described it, the law of privacy is "a thing of threads and patches."

GOVERNMENT CAN SPY ON YOU

WASHINGTON, D.C.—Robert Plamondon was charged with the dynamiting of a CIA office in Ann Arbor, Mich.

Plamondon and two other members of the Rainbow People's Coalition, also known as the White Panther Party, were charged with conspiracy to destroy the office.

During pretrial motions, government attorneys admitted overhearing the defendants on wiretaps which had not been authorized by a court order. The prosecutors asserted that no warrant was needed because a 1968 act of Congress authorized warrantless wiretaps to protect the national security.

Damon Keith, a federal district judge, ruled that the wiretaps were installed in violation of the 4th Amendment protection against illegal searches and seizures. He found that the 1968 law didn't permit warrantless wiretaps in purely domestic cases, but only when foreign elements were present.

The Justice Department took the case to the Supreme Court, which upheld the Keith decision in June 1972 by a vote of 8 to 0.

The government chose to drop the prosecution.

Another case involved Arlo Tatum, executive secretary of the Central Committee for Conscientious Objectors in Philadelphia.

After learning of the widespread Army surveillance of political dissidents in early 1970, Tatum and 12 other groups and individuals whose activities were recorded in a computer at Fort Holabird, Md., filed suit against Secretary of Defense Melvin Laird.

The plaintiffs included antiwar groups, civil rights attorneys and the garbage workers union in Memphis, Tenn.

Their case never came to trial. In June 1972 the Supreme Court decided, 5 to 4, that their complaint wasn't subject to court jurisdiction.

It wasn't enough for the plaintiffs to show that the system existed, Chief Justic Warren Burger wrote for the majority. They also had to show a "claim of specific present objective harm or a threat of specific future harm."

Legal scholars caution that sweeping conclusions shouldn't be reached from either of the decisions, but taken together they do constitute an important point to remember about your right to privacy: Within certain limits which aren't clearly drawn, your government can legally spy on you without telling you.

In general, federal, and some state and local, agents may conduct surveillance to protect the national security or combat crime.

Their judgments as to which individuals and organizations should be watched for those purposes sometimes, but not always, must be reasonable enough to convince a judge to sign a warrant.

In some cases, such as the Army surveillance of civilians, no judge is required to watch the watchers.

In any event, persons who aren't suspected of a crime or of threatening the republic may still have their utterances or activities recorded without their knowledge if they happen to have contact, however legitimate and innocent, with persons or groups under surveillances.

The laws, court decisions and administrative regulations governing the most common forms of surveillance aren't comprehensive, and their language is subject to interpretation and litigation.

The 1968 act cited in the Michigan wiretap case is the Omnibus Crime Control and Safe Streets Act. It permits the interception of oral and wire communications under three circumstances:

When a federal agency, acting through the attorney general, or a state or local agency acting through a prosecuting attorney, obtains a court order after revealing its reasons and plans to a judge.

All applications and installations must be reported annually to the Administrative Office of the U.S. Courts, which issues an annual statistical report.

Within three months after the expiration of a court order, a suspect must be notified that he was wiretapped. Judges may make transcripts available to the suspect.

When the president decides it is necessary in the interests of protecting national security. No court clearance is required, but the effect of the Keith decision is that some foreign element must be involved.

When a person in his private life is a party to the communication and is acting lawfully, or when he is a party to the communication and has previously agreed to be an informer for law-enforcement officials.

Mail privacy is governed by Postal Service regulations.

To open first-class mail, which includes most personal and business correspondence, a court order is required. But third-class and fourth-class matter may be opened without a warrant to see if postage requirements are being met.

Moreover, investigators for federal agencies may operate a "mail cover" if they can get permission from the chief postal inspector.

A mail cover involves the recording of any data on the outside of an envelope or package and an inspection of any mail other than first-class matter. It is supposed to be necessary for protecting the national security, locating a fugitive or obtaining evidence of a crime or attempted crime.

Other kinds of physical surveillance which don't actually trespass on an individual's home or office—such as cameras, or sensitive long-distance microphones—are legal whether conducted by government or private parties.

The effectiveness of the court-ordered variety of electronic surveillance has been questioned, most notably by Herman Schwartz, a law professor at the State University of New York at Buffalo.

The annual statistical reports show that about 2,700 installations have been authorized since 1968, with an unknown number of devices per installation, and that about 120,000 persons have been overheard in about 1.35 million conversations.

The reports also show that almost all the federal use of warranted tapping and bugging, and about half of the state use, is for gambling investigations.

That has occurred "despite the original claims that it was necessary primarily for serious crimes such as homicide, kidnapping and espionage," Schwartz said in a report for the American Civil Liberties Union.

On the other hand, Sen. John L. McClellan, D-Ark., chief sponsor of the 1968 act, has said the reports prove that wiretapping "is playing a key role in the war against crime."

The percentage of phone calls subject to court-ordered surveillance is "less than .0000039 percent," he told the Senate earlier this year. "The privacy of the average citizen, in short, is not threatened . . ."

(Most of the state wiretapping has occurred in New York and New Jersey. Minnesota officials have reported six installations since 1970.

(Last year Minnesota reported two phone taps, one for prostitution in Ramsey County and the other for narcotics in Hennepin County.

(One 1972 federal wiretap was reported in Minnesota, for a gambling and conspiracy investigation.)

The extent and effectiveness of national security surveillance, for which warrants aren't required, is unclear. The Nixon administration has put the figure at about 100 wiretaps annually. Schwartz estimates that these taps record large numbers of persons and conversations, because they are usually maintained for several months and frequently are on the phones of organizations, not individuals.

Even less is known about the use of wired informers, under the consent provision of the 1968 act. "All we know is that it is enormously used" and is probably the most common method of eavesdropping, Schwartz said in a telephone interview.

The use of consensual informers without a court warrant has caused at least one federal judge to voice alarm. Judge Gerhard A. Gesell of the District of Columbia declared in July, "Whatever incidental good flows from this invasion of privacy is submerged by the growing appearances of police surveillance so typical of totalitarian states."

Newly installed Attorney Gen. Elliot Richardson last month publicly specified in an unprecedented action, the criteria he will use in determining whether national security necessitates tapping and bugging. He pledged that he would balance the right to privacy with the needs of national security.

But that is a difficult balancing act, as Assistant Attorney Gen. William Ruckelshaus, who was acting FBI director, explained in a New York Times interview.

"Well, everybody agrees we shouldn't be conducting surveillance on a reasonable person. We shouldn't be using . . . surveillance on the political parties or on those extreme parties who are not violent but are just recommending a point of view . . .

"How you avoid getting into those other areas in the process of protecting against clearly illegitimate activities . . . is a very difficult problem and one that the society ought to spend a lot of time thinking about. The FBI ought to spend a lot of time thinking about it."

TAX RETURNS AND BANK RECORDS AREN'T ABSOLUTELY CONFIDENTIAL

WASHINGTON, D.C.—Early one morning last January a freshman Democratic congressman from Missouri Jerry Litton, sat in his office scanning the generally dull but occasionally revealing pages of the Federal Register, which publishes official government notices.

What Litton—a Chillicothe, Mo., cattle farmer—saw caused him to react as instinctively as if some witless bureaucrat had gone on record in favor of hoof-and-mouth disease.

Executive Order No. 11697, signed by President Nixon on Jan. 17 and published with accompanying Treasury Department regulations, authorized the Department of Agriculture to inspect farmers' tax returns "as may be needed for statistical purposes."

As Litton suspected, it was the first time the tax returns of an entire class of citizens had been opened up for any purpose, statistical or otherwise. "By noon he was raising hell and calling for hearings," an aide recalls.

Other congressmen began to raise hell, too, at what they considered an unwarranted and uncontrolled invasion of the privacy of confidential records.

Their eruption caused the issuance of a modified order, which is still in effect. But it wasn't changed enough to mollify the critics. Subcommittees of both the House Agriculture and Government Operations Committees have held hearings to determine what led to the order. They have determined that:

The order was, indeed, unprecedented, and involved the tax returns of about 3 million farm operators.

Despite its scope and uniqueness, the order was considered "not newsworthy" enough for a press release or other public announcement, an Agriculture official testified.

The original request from the Agriculture Department for access to the records was made three years earlier. Officials said they needed the information to prepare valid statistical samples for their crop and livestock reporting service and could obtain the information in no other manner.

Although Agriculture officials said they would use discretion and tight security in looking at the returns, the regulations isued by the Treasury were far from restrictive.

The broad language of the order and regulations was deliberate.

"The original order was prepared by the Department of the Treasury in language designed to serve as a prototype for future tax-return orders," Assistant Attorney Gen. Robert G. Dixon Jr. stated. Donald C. Alexander, Internal Revenue Service (IRS) commissioner, testified that if the order was a prototype, it would pave the way for mass inspections of tax returns by other departments of the federal government.

The hearings never determined exactly who decided to issue the controversial order, though Litton and others suspect some White House officials.

The Agriculture Department, under fire, hasn't yet used the access power, it is understood. Meanwhile, Litton and some 100 other congressmen have introduced legislation which would drastically restrict access to tax returns.

The case illustrates a fact of life: Tax returns—and other sensitive information such as bank and military records—aren't so confidential as many citizens might wish.

Alexander has suggested a reexamination of the laws governing disclosures of tax returns. For reasons which go back to the Civil War period, when tax information was published in newspapers, current law states that tax returns are public records, unless otherwise limited.

Access to the data, the IRS chief noted, is given to Treasury tax officials, to congressional committees, to states for tax purposes, to federal agencies "needing tax information for the accomplishment of their missions, and to federal agencies needing certain statistical information."

The information also may be furnished to taxpayers themselves, to their successors, executors of estates, legal partners and, in the case of corporate returns, stockholders owning at least 1 percent of the stock of a corporation. An American Civil Liberties Union (ACLU) survey of executive orders granting congressional committees and federal agencies access to tax returns shows that at least several dozen have been issued in the last 20 years.

The orders must state a purpose, such as an investigation. For example, the House Internal Security Committee, formerly the House Commitee on Un-American Activities, has been granted access during the 93rd Congress to "any income, estate or gift tax return for the years 1964 to 1974, inclusive" pursuant to any authorized investigation.

The semiannual IRS report on inspections of tax returns indicates that some 20,000 returns were looked at by other federal agencies in the first half of 1973. More than half of those were seen by the Justice Department.

Allegations that audits of tax returns were used by the Nixon administration to punish its political enemies are being investigated by a congressional joint committee.

Congress also is taking a new look at the confidentiality of bank records, particularly the power of law-enforcement agencies to look at microfilm records of checking-account transactions without obtaining a subpoena or notifying the account holder.

Legislation has been introduced in both houses to amend the 1970 Bank Secrecy Act, which was designed to curb illegal use of secret foreign bank accounts and to make it harder to commit white-collar crimes such as tax evasion. At Senate hearings last year Treasury and Justice Department officials vigorously opposed any additional restrictions on access to bank records by investigative and law enforcement agencies.

They admitted that banks don't always require an agent to show a subpoena or any other official permission to gain access to records, and that account holders frequently don't know that their transactions have come under scrutiny. Eugene T. Rossides, assistant Treasury secretary, said it would be "cumbersome" to obtain a subpoena in many cases, because agents rarely show a probable cause for inspection.

In any event, he said, there is no privacy issue at all involved in inspecting bank records. A Justice Department official contended that the account holder has no proprietary interest in his records and no protection under the Fourth Amendment against illegal searches and seizures. Rossides said he "did not see that there have been examples of abuse" in the surveillance of bank records.

At the same 1972 hearing, however, newspaper columnist Jack Anderson and an ACLU spokesman submitted examples which, they said, showed that the records of persons who had committed no crime but had espoused unpopular causes had been searched by the FBI without any subpoena. The examples included actress Jane Fonda, black activist Floyd McKissick and the Unitarian-Universalist Association, a religious body.

"Those who take comfort and say, 'Yes, Jane Fonda and Floyd McKissick have to be investigated,' may find themselves being investigated," warned Anderson. "George McGovern might win, and maybe he would put Ramsey Clark in as head of the FBI, and instead of investigating Jane Fonda they will start investigating John Wayne."

The reporting provisions of the Bank Secrecy Act and the regulations issued to implement the law were challenged in a court suit by Fortney H. (Pete) Stark, a California banker.

A federal district court held some of the provisions unconstitutional, and the case is on appeal before the Supreme Court. Stark, meanwhile, has been elected to Congress and is a major House sponsor of the restrictive legislation, which also is supported by banking organizations.

The confidentiality of other types of highly personal data held by the government ranges from tight to loose. Census data is tightly secured, generally available only in the form of aggregate statistics. Individuals may obtain census information which they submitted, but only by going through a clearance process.

Social Security information, which can be useful in pinpointing the whereabouts of most wage earners, is regarded as confidential. With few exceptions, it isn't available to law-enforcement officials, private detectives, bill collectors or persons searching for errant spouses.

Military personnel records are much more widely available. They are open to the Civil Service Commission if the individual applies for federal employment.

They are also available under Justice Department directives to enable the conduct of business of the Defense Department; other federal, state and local agencies including all levels of the legislative and judicial branches; "and in such other instances where release is clearly required by the national interest."

Computers and Privacy

WASHINGTON, D.C.—About two years from now, if all goes according to schedule, the city of Wichita Falls, Texas, (pop. 116,000) will have a fully operational, computerized municipal data and management system.

It will contain up-to-date, easily retrievable information on "any kind of business a citizen does with the city," said Jerry Dunn, assistant city manager.

Police records, health records, data on the ownership and value of land parcels, and utility accounts will make up most of the information base.

The Wichita Falls system is one of several in a pioneering federal research effort to enable cities to speed up the flow of the thousands of pieces of data that travel within government, make the data timely and accurate, and provide it quickly to help make decisions or solve problems.

Such mundane chores as the filling of street potholes may be accomplished quicker and at less cost, developers of the system believe.

But comprehensive data systems also raise questions about the protection of confidential information, and how it might be misused.

"There has been a lot of misunderstanding, particularly at the federal level, and some innuendo that we're building a Big Brother system," Dunn said.

"That couldn't be farther from the truth. What we're trying to do is just improve municipal government," he said.

Wichita Falls has come to grips with the privacy issue at least in part, because it had to under terms of the federal program.

A city ordinance, passed about 18 months ago, was believed to be the first in the country to regulate the dissemination of confidential or sensitive data that will be stored in the system.

The ordinance created a Data Access Advisory Board and a data registrar to oversee daily operations.

Charlotte, N.C., also is establishing a comprehensive data system with privacy safeguards under the guidance of the federal Urban Information Systems Inter-Agency Committee (USAC).

Both cities are getting federal money to help set up the demonstration systems. Three other cities—Dayton, Ohio; Long Beach, Calif.; and Reading, Pa.—are creating specialized systems in the areas of public finance, public safety and physical-economic development.

A sixth city, St. Paul, was chosen to develop a human-resources information system, but the project foundered and was ended last year.

Robert A. Knisely, USAC chairman, freely concedes that computerized data systems have "the potential for some horrendous privacy problems" but he is also a pragmatist.

"There's no profit in saying that computers can be stopped," he said in an interview. "So it's up to people of good will to see that they do only what they're intended to do."

The current climate of heightened awareness and concern over the privacy-invading capabilities of computerized data banks dates back at least to 1965 and a proposal for the establishment of a National Data Bank.

The proposal to coordinate the preservation and use of socio-economic data aroused strong opposition in the press and among lawmakers. Both houses of Congress held hearings, and the idea eventually was smothered in a blanket of protest.

The realization that the computer would make it much easier to record, store, retrieve information—and, perhaps, integrate it into comprehensive personal dossiers—stimulated newspaper and magazine articles. Books, such as "Privacy and Freedom," by Alan F. Westin, and "Assault on Privacy," by Arthur R. Miller, sounded the alarm.

The articles and books reported various plans for sophisticated data banks of the kind which raised Big Brother worries.

In the fall of 1973, however, there are no such data banks in operation, according to a number of privacy experts interviewed by the Minneapolis Tribune.

Westin, a Columbia University professor, put it this way:

"In the sense that you're talking about a whole level of a government having merged its files into one common data base, there's no such omnibus data bank anywhere in American government today."

However, he added, there are some in which a few files are merged and there will be more, particularly at the state level where there is pressure to economize on the use of costly computers.

The concerns of the late 1960s led to some extensive studies in the early 1970s.

The Senate Constitutional Rights Subcommittee, chaired by Sen. Sam Ervin, D-N.C., is completing a four-year survey to determine the extent and nature of personal data collected and stored by federal agencies.

The survey has grown to include 54 departments, offices and agencies which have about 750 personal data files of various sizes and contents.

Ervin noted recently that the Office of Emergency Preparedness (OEP) reported the existence of a file on 5,000 individuals but said it had no access to the contents and didn't know what information was contained. The OEP said it maintained the file for the White House, whose personnel operations specialists had exclusive access.

The Canadian Departments of Justice and Communications issued a report earlier this year based on a study which "revealed a network of information paths linking the bureaucratic structures, both public and private.

"In brief, more personal information is being collected than most Canadians probably suspect, and is made available to a larger number of users than is probably supposed. There is no evidence that either of these trends will decline," said the report, "Privacy and Computers."

"Databanks in a Free Society," a report compiled by Westin and Michael A. Baker for the National Academy of Sciences, studied the use of computerized record-keeping by 55 commercial, government and non-profit organizations in 1970 and 1971.

The study was undertaken to determine whether the growing use of computerized records was injuring civil-liberties interests as many experts, including Westin, had predicted.

Westin and Baker reported finding no abuses of the kind that had been widely feared. If anything, they said, computerized records were more objective, less sensitive and more secure than manual records.

They were surprised by their findings, they said, stressing that their observations were based on what they had seen and not on what might occur in the future.

In August a citizens advisory committee to the Department of Health, Education and Welfare (HEW) completed on extensive study and issued a report, "Records, Computers and the Rights of Citizens."

Finding that, "under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices," the committee recommended enactment of a federal "Code of Fair Information Practices" and other safeguards against inaccurate records and improper dissemination.

The committee was opposed "at this time" to the growing use of the Social Security number as a universal personal identifier.

It also concluded that the possibility of assembling information from various data banks into one comprehensive dossier on anyone is currently remote because of technical reasons. "Nonetheless," it added, "public concern . . . is well-founded."

A special subcommittee of the Minnesota Senate has announced it will hold hearings soon on privacy and computers. Legislation to control the collection, storge, dissemination and use of personal data by state agencies passed the Minnesota House in the last session but was stalled in the Senate. It is being readied for reintroduction at the next session.

Among experts in the field, there is general agreement that computerized records can be protected from intrusion better than manual files, although enough time, brains and money can crack the security of any computer system.

Robert P. Henderson, a vice-president of Honeywell Inc., who has spoken widely on security and privacy, has warned that "the staff of a data processing department is still the weakest link in a security chain, for it is the staff that has the technical ability and the best opportunity to tamper with the system or secure sensitive information."

On the other hand, David B. H. Martin, an HEW official who served as executive director of the advisory committee privacy study, pointed out in an interview two inherent safeguards against excessive abuses in computerized record-keeping.

One, he said, is the demonstrated incompetence of large bureaucracies to carry out anything complicated, such as the compilation of Big Brother-type dossiers.

The other, he said, is the ability of small groups of individual citizens to foul up a computer system through the legendary tactics of folding, spindling and mutilating.

Confrontation in Massachusetts

Boston, Mass.—"Today the citizens of Massachusetts won a major battle with the federal government," Gov. Francis W. Sargent announced Sept. 25.

"I say major for there is no greater issue today than the right of the individual to be protected from all unwarranted invasion of his private affairs.

"Today I have been notified that the Justice Department will drop its lawsuit against Massachusetts. That suit attempted to force this state to feed unprotected private information into the national criminal data bank," Sargent said.

Both the Justice Department's decision to drop the suit and Republican Gov. Sargent's earlier decision to fight Washington over the matter of disseminating criminal records signified movement on an important public-policy question.

The Justice Department was tacitly admitting that better safeguards are needed as a national, computerized criminal history system builds toward full operation.

Sargent was showing that, in Massachusetts at least it is now perfectly respectable and perhaps politically profitable for an elected official to make privacy a major issue.

The aborted legal struggle stems from a 1972 Massachusetts law, the first of its kind in the nation, which provides strict accuracy and confidentiality safeguards on computerized criminal records in the state.

In brief, the law bars the inclusion of "intelligence" data; provides for the retention of records only upon conviction, not just because of an arrest; provides legal procedures for individuals to inspect, challenge and correct or expunge the information contained in the record about themselves; and limits access to the files to police, court and correctional officials, or to other agencies specifically authorized by statute.

Last June, as Massachusetts prepared to link up with the FBI's National Crime Information Center (NCIC) computer data bank, Sargent announced that the state wouldn't join because NCIC's computerized criminal history file, one of eight files in the total system, lacked the safeguards of the Massachusetts law.

"We have been careful in Massachusetts," Sargent declared, "but what good are our controls, our safeguards . . . once we plug into this uncontrolled national system?"

At the same time, the Justice Department filed suit on behalf of the federal Small Business Administration (SBA) and the Defense Investigation Service, both of which had been denied access to the Massachusetts files. SBA threatened to withhold $30 million in loans to Massachusetts residents unless it was allowed to check loan applicants for criminal records.

The defense agency held up clearance of 2,400 defense-related jobs in Massachusetts; it was attempting to check the backgrounds of defense contractors' employees.

Early in August, Sargent's cousin, Attorney Gen. Elliot Richardson, foreshadowed the abandonment of the Massachusetts suit by announcing that a Justice Department task force was drafting comprehensive security and privacy legislation. The disclosure was made in a letter to Gov. Robert R. Ray of Iowa, another state which passed safeguard legislation.

The FBI's NCIC contains records on wanted persons, stolen vehicles, guns, securities, boats and other items, but its computerized criminal-history file is the focus of controversy.

It is only in partial operation. As of Aug. 1 there were 378,000 criminal histories in the computer. Just six states—Illinois, Arizona, New York, California, Florida and Pennsylvania—and the District of Columbia are full members contributing information.

Ten federal agencies also submit and withdraw data. Thirty-seven other states can only withdraw information. (Minnesota isn't expected to become a full member for at least two years.)

The FBI has disclaimed responsibility for the accuracy or the use of the information in the computer. FBI officials say that is the responsibility of the states and agencies which use it.

Norman Stultz, the agent in charge of NCIC, said in an interview that the criminal history computerization, put "on line" late in 1971, isn't expected to be operating nationwide for at least two years. Eventually, it will contain millions of records.

He said the file doesn't contain so-called intelligence information, that it excludes records of some minor offenses such as disturbing the peace, that each record is accompanied by a fingerprint for positive identification and that very few of the records predate 1970.

Critics of present federal and state criminal record practices don't deny that the records are needed for criminal-justice purposes.

They contend, however, that the practices are sloppy at best. And at worst, individuals are denied the right to go to school or earn a living because of a possibly erroneous or incomplete record.

They charge that arrest records often aren't updated to show the disposition of the case, an allegation law-enforcement officials agree is true.

In cases where no conviction was obtained, arrest records should be wiped out, the critics say. Law-enforcement officials strongly disagree with that.

The critics make several points:

According to a 1967 report of a presidential commission, the probability of a black urban male being arrested at least once in his lifetime is as high as 90 percent. For white urban males it is 60 percent, and for all males, 47 percent. Yet fewer than 25 percent of those arrested per year are found guilty.

The Supreme Court, in a 1957 decision, held that "the mere fact that a man has been arrested has very little, if any probative value in showing that he has been engaged in any misconduct. An arrest shows nothing more than that someone probably suspected the person apprehended of an offense."

The record of an arrest, however dubious, has deprived persons of jobs. In a test case filed with the help of the American Civil Liberties Union, a man named Dale Menard ued to remove his arrest record from FBI files and prevent its dissemination to potential employers.

Menard had been arrested in Los Angeles for suspicion of burglary, but was never prosecuted. There was not clear evidence that a crime had been committed by anyone.

In June 1971 a federal district judge ruled in favor of Menard and ordered the FBI to stop disseminating arrest records except to law-enforcement agencies for law-enforcement purposes. Judge Gerhard Gesell said the system was "out of effective control."

Congress quickly passed legislation to override the dissemination order. The question of removing the record altogether is before an appeals court.

At his Senate confirmation hearing, new FBI director Clarence M. Kelly resisted suggestions that arrest records shouldn't be maintained, or that they shouldn't be disclosed without updated information on the status of the case.

Kelly said arrest records are "very helpful" in police investigations. Knowing the dispositions of arrests, he said, would be desirable "but it is practically impossible, and economically it is extremely expensive" to check with an arresting agency.

Another major criticism raised against criminal-record practices is the abusive distribution of the information to persons outside the criminal justice field.

When Kelly was police chief in Kansas City, his department operated a regional, computerized criminal information file.

An excessive number of inquiries to the computer were being made from nearby Lenaxa, Kan., and it was found that the Lenaxa police chief was running police record checks on newcomers to town for the benefit of landlords and employers.

Since Massachusetts tightened access to its criminal records it has turned down requests for information from dozens of sources, all of which apparently obtained arrest records and other data before.

They included city and state officials and regulating agencies, private and public child care agencies, an adoption service, military recruiters, private detectives and insurance claims adjusters.

Persons listed in criminal-record files should at least be able to inspect the information, challenge it and cause it to be corrected or updated, the critics also say.

That many records are inaccurate or outdated was demonstrated when Massachusetts began to convert its manual files to the computer. A spot check of 1,000 purported conviction records showed that 20 percent didn't involve convictions.

Arnold Rosenfeld, chairman of the state's Criminal History Systems Board, said the error rate "blew everybody's mind, and all of our board members are law-enforcement and criminal-justice people."

Although one fight between Massachusetts and Washington is finished, another one continues.

In this battle, Massachusetts has balked at supplying certain information on the treatment records of drug users because state officials believe it could be used to identify persons who seek treatment.

Federal officials who run the Client Oriented Data Acquisition Process (CODAP) have said the disputed information is needed for efficient management to identify any duplication of treatment.

But Massachusetts officials fear the identification elements could be used to compile records that would place a lifelong stigma on persons who seek drug treatment.

The state has negotiated a temporary agreement with federal officials to omit the disputed information—the day and birth date of the person and the initials of the mother's maiden name.

LEGISLATIVE SAFEGUARD PROPOSAL

WASHINGTON, D.C.—Two years ago, as Bill McClaine and his boss were visiting the Los Angeles FBI office, the agent in charge showed them a machine that he said was linked to intelligence files. Acting on an impulse to demonstrate the system, the agent asked McClaine for his California driver's license number and punched it into the Teletype machine with some other information.

Back came several pages of highly confidential information on Bill McClaine, administrative assistant to Rep. Barry Goldwater Jr., R-Calif. It amounted to a dossier, according to McClaine, including his places of residence, annual income, home mortgage data, driving, employment and family histories. "It had everything," McClaine said recently.

Some of the information went back 10 years to when he underwent a top secret national security clearance as a Coast Guard officer, but it also contained up-to-date intelligence. To this day McClaine isn't certain where the dossier was stored, but he believed it was in a California state computer system created with federal money.

McClaine did have security clearance at the time of the incident, but he had never been arrested, and the discovery that an FBI office could get so much confidential information on him so quickly shocked him.

More importantly, it also made an impression on Goldwater. Young Goldwater, son of the Arizona senator, has become a congressional sponsor of privacy legislation. And this summer, when several liberal lawmakers and organizations petitioned the Justice Department for tighter controls on the FBI's criminal records system, Goldwater Jr. put his conservative name on the petition.

Lawmakers from Goldwater on the right to Rep. Bella Abzug, D-N.Y., on the left are showing enhanced interest in the subject of privacy these days. With a big assist from the Watergate scandal, privacy legislation has risen from the lowest ranks of congressional concerns to become a more visible bipartisan cause. "You've got the whole political spectrum talking about this, not to mention Weinberger and Richardson," said one Capitol Hill aide.

Caspar Weinberger, secretary of Health, Education and Welfare (HEW), and Elliot Richardson, attorney general have promised that their departments soon will put forth proposals for new privacy safeguards. Advocates of stronger privacy and confidentiality measures both inside and outside government say they believe the climate is right for passage of new laws. But they are chary of predicting when that will start to happen or the form the laws will take.

Basically, there are two possible legislative approaches. One is to attempt to regulate all government record-keeping systems via a single bill, such as one that has been introduced repeatedly in recent years by Rep. Edward Koch, D-N.Y.

The Koch bill would require any record-keeping government agency to:

Notify everyone in its files of the existence of the files—a requirement which even the advocates of the Koch approach say would be prohibitively expensive.

Maintain detailed records whenever information from the file is given out.

Allow each person to inspect, challenge and correct records about himself.

The Koch bill would exempt "national security" data, law enforcement investigatory files and certain agency letters and memoranda. It would establish a Federal Privacy Board to hear and rule on citizen complaints.

A recent report of an HEW advisory committee, "Records, Computers and the Right of Citizens," recommended enactment of a federal Code of Fair Information Practices for all automated personal data systems. The code is based on the principle that citizens should be able to find out what is recorded about themselves, be sure the information is used for the purpose intended, and correct it if it is inaccurate.

The second approach is to enact separate laws to deal with specific surveillance and record-keeping problem areas.

The Fair Credit Reporting Act, which became law in 1971, could be a model for other laws. That act gives consumers a limited right to learn what is in their credit files and correct any misinformation; Congress is considering amendments to clarify and strengthen the consumer's position.

Specific subjects of bills introduced by various lawmakers include Army surveillance of civilians, criminal arrest records, mailing lists, prohibition of the Social Security number as a universal identifier, prenotification of bank customers whenever law enforcement authorities seek to examine records of transactions maintained by banks, and outlawing the recording of phone conversations unless the other party has been told about it.

There are other ideas in the congressional hopper, too. For example, Sen. Gaylord Nelson, D-Wis., has urged the creation of a congressional Joint Committee on Individual Rights.

Committee jurisdiction is a problem which could retard or prevent the passage of privacy legislation. A number of committees and subcommittees can claim jurisdiction over pieces of the privacy pie—Banking, Judiciary, Government Operations and the taxation committees, among others.

Some influential initiative to get legislation moving could come from Sen. Sam Ervin, D-N.C., when he completes his assignment as chairman of the Watergate investigation committee. Impetus also could be provided by the Justice Department, which is currently trying to pilot new regulations and proposed legislation on criminal records through the turbulent waters of the administrative bureaucracy.

The Justice agency may attempt to develop a series of privacy bill for introduction in 1974, based on its responsibility for administering the Freedom of Information Act.

The Minnesota Legislature this year considered but failed to pass legislation that would set standards and guidelines for the collection, storage, dissemination and use of sensitive personal information by state agencies.

The bill, modeled after a recently enacted Swedish law, would cause the commissioner of administration to issue rules and would create an appeals committee to rule on the accuracy and relevancy of data kept by the agencies.

Violations would be a gross misdemeanor under the bill, which passed the Minnesota House but stalled in the Senate. The proposal is being studied and readied for introduction in the next legislative session.

[From the New York Daily News, Mar. 25–27, 1974]

THE RAPE OF PRIVACY

(By Michael Pousner)

SOMEWHERE THERE'S A FILE ON YOU—ITS DATA COULD BE FALSE—IT COULD HURT YOU—BADLY

"As every man goes through life, he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from each man, millions of threads in all. If these threads were suddenly to become visible, people would lose all ability to move."

—Alexander Solzhenitsyn,
"The Cancer Ward"

Imagine living in a country where 131 million citizens are the subjects of private dossiers delving into their livelihoods, family life and frequently their manner of living.

Imagine living in a country where 54 national agencies have over 750 data banks containing extensive information on almost all of its adult citizens.

Imagine living in a country where a universal numerical identifier may one day follow a citizen from crib to grave—recording for posterity any purported sins committed along that path.

That country is not Solzhenitsyn's native Russia, but the United States, where privacy, "the most prized but the most perishable of our civil liberties," as Sen. Sam Ervin (D–N.C.) puts it, is now under unprecedented assault.

"I personally feel the right to privacy is now in danger more than anytime in this century," notes Sen. William Brock (R–Tenn.), a member of the Senate Consumer Credit subcommittee.

"Congress and the American people in general are only now becoming aware of the multitude of the ways in which our right to privacy—our right to be left alone—is being compromised by the collection of information about almost every aspect of our daily lives," adds Ervin, who has been holding hearings on the issue over a four-year period.

Threats

President Nixon also has come to see the problem. In February he announced the appointment of an 11-member panel chaired by Vice President Ford to examine the threats to privacy and recommend procedures to protect it. By June, the panel is to begin presenting "a series of direct, enforceable measures that can be immediately put into effect."

The increasing governmental concern is well-founded. In the past, after all, privacy problems seemed the domain of radicals of all stripes, credit wastrels and general ne'er-do-wells. Keep your nose clean, the feeling used to be, and you won't have any problems.

Today's information explosion, however, threatens to consume the privacy of every American. Just ask yourself about the daily footprints you casually leave behind:

Have you applied for auto insurance or a job recently? If so, credit and character reporting snoops may well have tried to get to know you—though not personally—to get to know everything about you: your neighborhood, your salary, what your neighbors and fellow employes think of you; the way you keep your house, the state of your marriage, even your drinking and sexual proclivities—all in the name of determining your employability or insurability.

More than 2,500 credit reports on over 100 million Americans, and quite often, Congressional testimony has revealed, the information is misleading or totally false (see footnote 1).

Do you own a car? If so, your name, address, and car type have been sold by the New York State Department of Motor Vehicles to a Detroit firm for mailing list purposes.

Have you ever been arrested, even for a traffic violation, say, or for something as innocuous as streaking? If so, even if you weren't convicted, your record may tick away like a time-bomb in some file which may already have been plugged into a federally-funded national computer data bank. And the FBI is currently computerizing criminal records, raising the spectre of a man being forever the prisoner of his record.

Have you applied for life insurance? If so, your so-called confidential medical record, as well as additional information about the way you live, is probably on file in an insurance data bank. The Medical Information Bureau of Greenwich, Conn., alone has the records of 12 million insurance applicants available to over 70 insurance companies.

If the White House plumbers had known about these medical data banks, said Sen. William Proximire (Dem-Wisc.), only half-jokingly at recent Senate hearings, there would have been no need to break into the office of Daniel Ellsberg's psychiatrist.

Have you been hospitalized for physical or emotional disorders. Increasingly, companies routinely lateral that information over to computerized credit data firms.

---

[1] The Strange Case of James Millstone.

When James Millstone moved back to St. Louis after working as a St. Louis Post Dispatch Washington correspondent, he routinely informed his insurance broker to switch his auto insurance to a local company.

The application was rejected by the new company.

Millstone—a fortyish father of four with an excellent driving record—was befuddled, but many angry letters and threats of legal action later he discovered the reason for the rejection. The credit reporting firm hired by his insurer had come up with the following information on him:

He was reported to be a "hippie type," suspected of being a drug user, had a history of apartment evictions, was troubled by a lack of judgment and a bad attitude, participated in a peace demonstration, was disliked in his neighborhood, and had unruly and uncontrollable children.

All suggestions that weren't silly were patently false—the product of either a credit investigator's fertile imagination or an interview with the one neighbor in the quiet Northeast Washington neighborhood with whom the Millstones didn't get along.

Interestingly enough, no dirt was uncovered about Millstone's driving record—which was what the investigation was supposed to be all about.

Millstone eventually got the insurance, but is suing the credit firm for damages, contending additional fallacious and potentially damaging information remains in his files.

Unfortunately his case is far from unusual.

Have you been hospitalized for physical or emotional disorders. Increasingly, cities are putting this information on tapes into centralized data banks.

Do you subscribe to magazines, give to charities? Companies bandy about these mailing lists like kids trading baseball cards.

Commenting on the whole trend toward data collection, a report from the Massachusetts Special Commission on Privacy and Data states:

"This personal information may be collected without the consent of the individual; without provision to check its accuracy; and without control over its dissemination."

Disastrous

Even civil libertarians who perpetually fret over the erosion of individual rights concede little wrong with computerization of records per se. They are alarmed, however by the potential cross-pollination between governmental, credit, and medical data banks utilizing Social Security numbers—now required by almost all banks, businesses, schools, and even airlines and hotels—as universal personal identifiers.

Further, computers err no less than humans and their forgiveness is rarely divine—a fact attested to by anyone who's ever received the umpteenth threatening notice from a store whose bill he paid months before. And when a criminal records computer, for example, makes a mistake, the consequences are potentially disastrous.

There's a former Marine deserter from Texas who served his military prison time and was discharged. He has been picked up and detained three times in the past year alone because the computer still lists him as "wanted."

Then there's the young couple from San Francisco, Calif., who were detained by police for 18 hours because they were driving their own car that was stolen but had been recovered. Someone forgot to tell the computer.

In the credit and character investigation areas where, critics insist, much of the information is based on hearsay anyway, computer errors tend to become sanctified. And, as experience has repeatedly shown, the wrong people have an amazing ability to obtain that information. Some credit firms will give out information about you over the phone to anyone calling and identifying himself as a potential employer.

To some experts, the most insidious threats to privacy come from well-meaning bureaucrats who can't resist the temptation to categorize, catalogue and classify us. Earlier this month, for example, it was revealed that the federal government is planning to set up a computerized data bank with educational, ethnic and family information about more than 100,000 of the city's elementary school pupils. Another federal effort—this one to computerize local students' attitudes about race—was beaten back last week only after heated local objections.

In almost every case, the privacy abusers can present well-reasoned arguments supporting their efforts. But the road to 1984 is paved with good intentions. Said Supreme Court Justice Louis Brandeis in a famous 1928 decision: "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."

How Brian McGraw Was Left for Dead

The so-called "private dossier industry" is massive and always growing like Topsy, so it's not surprising that, as consumer advocate Ralph Nader notes: "It's a rare American who does not live in the shadow of his dossier."

But for most Americans, their dossiers are just that. A shadow. Only a potential threat to their credit ratings, community standings and financial well-being.

For a significant number of innocent citizens, however—victims of fallacious credit and character reports, of unsubstantial gossip, of classic computer foul-ups—the dossier shadow can darken their entire life.

These victims are the casualties of the war on privacy, bearing critical, festering wounds; careers shattered, families fractured, credit ratings devastated, community standings irreparably harmed and, above all, almost inevitable emotional injuries. The bewildering feeling of finding oneself trapped in a Kafkian maze from which there is no escape, nowhere to turn, no one available to answer their life-and-death question: "Why me?"

A New Jersey man we'll call Brian McGraw daily asks himself that question—and with good reason. For 12 years he has been haunted by a fallacious character investigation report.

CRUSHED

Even today, as his $750,000 suit against the company that investigated him finally heads to court—his problems continue. His case seems solid, but there is no precedent for $750,000 judgments in that particular legal area. Whatever money he wins can hardly make up for what has happened to him.

Brian is 43 now. The hair is greying, thinning, the face fleshy. The spirit appears crushed. The mind, however, remains alert as he sits behind the kitchen table of his austere apartment and tells his story in an unemotional monotone.

But when he mentions the company that looked into his life, his eyes narrow and his voice rises. When he talks about his family, he occasionally flicks a tear from his eye. Unobtrusively.

To play on a current phrase, Brian McGraw knows where he was in '62. To many people the year conjures up dim memories of the Cuban Missile Crisis and kids in motorcycle jackets lounging around juke boxes. But to McGraw—then 31, a newlywed with a zillion dreams and aspirations—1962 was the year when something began to go drastically wrong in his life.

ENTHUSIASTIC

McGraw had spent several years in a desk job for a large cosmetics firm. By all accounts, he was well-regarded, but he wanted to get into sales—the requisite step to middle management.

No openings seemed imminent, so he quit and, armed with good references, interviewed at a larger, competing firm which offered sales possibilities and a higher salary.

After the initial interview and tests, the sales manager informed him enthusiastically that he scored higher than anyone who had ever taken the tests and immediately offered Brian the job. Brian accepted.

Several days later, Brian was called in by the suddenly grim-faced sales manager and told to "come clean" about the information on his job application. Brian had answered all the questions truthfully, and didn't know what the man was talking about.

Within weeks, things went from okay to bad to worse at the firm—poor assignments and finally trifling desk work again—and six months later Brian quit.

"I was young, innocent," he reflects. "What the guy said about coming clean bugged me, but I just thought he was something of a kook and passed it off."

He took another job—a lower-paying position for which he was over qualified as the new firm's only college grad—and looked around for other positions.

Nothing. And for four years, he seemed to be viewing reruns of that depressing scenario. Warm reception at initial interviews. Then sudden notification that "open" positions had already been plugged. "Unanticipated hiring freezes." "Qualifications aren't right for the position."

Brian began doubting himself. Maybe he presented a bad impression. Maybe he had nothing to offer a potential employer.

OPPORTUNITY

In the back of his mind was that "come clean" admonition from the cosmetics man, but he never knew what to make of it.

In 1967, finally, an encouraging employment development. Again Brian was overqualified but at least the new job offered a long-range opportunity to get into sales. At this time, though, his wife was pregnant with their second child and very sick. The job entailed an immediate move to another state. Reluctantly Brian turned it down—a decision he rues to this day.

Strangely enough, on the very day he turned down the job offer, rendered by the firm's district manager, Brian went home to find a form letter from the company's central office informing him that Company Z "has no vacancies."

That did it. The next day, Brian demanded an explanation. The district manager called the central office and, aghast, turned to Brian.

"I like you Brian, you can tell me," the manager said soothingly, "What is it? Are you a homosexual or a criminal?"

Brian is most certainly neither. Now it all seemed clear. Some unknown force had been sabotaging his career. But agitatedly pumping the sales manager for

further explanation was fruitless. The man feared he'd already told too much.

For nights on end, Brian walked the streets aimlessly. "I was climbing the wall," he says, "I feared for my wife, my family, my future. I didn't know what it was all about."

Finally, he consulted a lawyer. In five minutes, the lawyer was able to find out the information that eluded Brian for five years.

A credit reporting company had been hired by the cosmetics firm in 1962 to conduct a "routine" pre-employment character investigation on Brian.

It alleged—and all the companies accepted as the gospel—the following "facts:" Brian had been dishonorably discharged from the Navy (the most damaging allegation). During a "noisy late night party" in 1962 a neighbor had called police to complain, and, after the cops left, Brian and his wife stormed into this old lady's apartment, although they allegedly knew she was very ill. Brian spit on her and his wife cussed at her, and the lady took them to court. Even after that incident Brian continued to be "rude, abusive, and scurrilous" at every opportunity. When he moved out, the landlord was glad to see him go.

The truth: honorable discharge; no noisy late parties; it was the lady, neighbors said, who was disliked in the neighborhood.

Further, Brian and his wife, tired of the lady's harrassment had taken her to court as well (both cases were dropped). Brian's landlord signed an affidavit that the McGraws were excellent tenants.

TRAVAILS

Although his file hadn't been updated since 1962, those misentries alone were sufficient to sink Brian's dreams.

Unfair? You bet. Uncommon? Not at all. Congressional testimony and letters to the Federal Trade Commission have revealed extensive abuses of bad-information hungry credit-reporting firms that have ruined many Brians.

The Job-like travails of Brian McGraw continue to this day. While Brian was having his problems, younger men with "cleaner" records were moving rapidly up the sales ladders. And few employers seem interested in a guy with Brian's past problems—even though he is innocent.

Brian's attorney, noted New York lawyer Harry H. Lipsig, puts it quite succinctly: "Brian was raped."

Slamming the Door on Snoops: Step 1

As never before, each American's right to privacy is like a frail tree buffeted by hostile winds. A push here, a shove there—and privacy topples.

Auto and life insurance, as examples, provide a family with a safer seat for negotiating life's bumpy turns. Business loans and retail credit also smooth the journey. And the possibility of secure employment keeps society healthy.

But each year, to their chagrin, millions of people fall off the merry-go-round. Routinely applying for insurance, employment, loans or credit, they unexpectedly receive the thumbs-down or "high-risk" routine.

If you're one of those people, your first tendency is to track your memory. You've always paid your bills on time. Your health is fine. Good employment. Driving record okay.

So what's the problem? You may very well be the victim of inaccurate personal information generated by an information-collection firm hired to check you out.

Solution: For the moment anyway, throw up your arms, wring your hands and reach for the crying towel.

At least that seemed to be the conclusion of a landmark study released last year by a blue-ribbon Department of Health, Education, and Welfare citizens privacy commission.

"Under current law," the study noted, "A person's privacy is poorly protected against arbitrary or abusive recordkeeping."

REFUGE

True, there is one refuge for the abused person—the highly-touted Fair Credit Reporting Act, passed by Congress in 1971 in the wake of thousands of consumer complaints about inaccurate and unfair credit reporting.

And to some extent, privacy experts agree, the FCRA has helped. Consumers can find out which credit-rating and character-reporting firms are blackballing

them; can demand a recheck of their dossiers; can require the firms to take out inaccurate information or have their own sides of the story printed in their dossiers; can sue for certain damages.

At least that's what the law says.

But the FCRA is far from perfect, as even the Federal Trade Commission, the governmental agency charged with enforcing it, concedes. Sheldon Feldman, a top FTC official, recently told a House hearing that "the Fair Credit Reporting Act has not fulfilled its goals."

Bulging FTC complaint files and press accounts of growing new abuses from the "credit victims' Hall of Fame" bear out his statement. To list a few:

A Richmond, Va., woman is suing 10 insurance companies for $21.6 million because she was allegedly put in a "high-risk" auto insurance category for—gasp!—"practically living with a man," a charge she terms "meaningless gossip."

A Princeton University faculty member was denied insurance allegedly because of a report that she was living with a man to whom she wasn't married.

A mid-Western university professor discovered his potential elevation to department head stymied and his career on the decline after a credit-reporting firm told the university that his wife had a terrible drinking problem. Untrue. In actuality, she barely qualifies as a social drinker.

There also seems to be an increase in the number of classic credit-reporting computer snafus, so easily perpetrated and so hard to eradicate. A Cambria Heights, Queens, man has been rejected for credit at a number of local banks because bank computers continue to confuse his credit history with that of his father.

The nature of credit-reporting itself has been left substantially untouched by the law. Surveys show that most Americans agree that insurance companies and potential employers have thhe right to run SOME check on us.

But who needs them snooping around our neighborhoods, prying into our bedrooms, quoting people who barely know us—and, as some critics charge, actually manufacturing information about us?

STRENGTHENING

The "disclosure" provisions of the FCRA have also come in for their share of criticism from officials like Sen. William Proxmire (D–Wis.) who has been holding hearings on strengthening the bill.

Although the FCRA allows a consumer "access" to his dossiers, the investigating company is not required to actually let him look at the entries—and usually doesn't. Entries are usually rendered in verbal or written summaries, leaving the consumer to wonder whether he's been given the whole truth. Also, the present act exempts character snoops from revealing what medical information a company may have on you—one of the fastest growing areas of abuse.

Great ambiguity also remains about what information is erroneous and therefore "deletable." "It's like pulling teeth to get those companies to retract information," is how one local attorney told me.

When one privacy victim, for example—turned down for insurance for a welter of fallacious reasons—met with officials of the company to correct his record, he says he still found them reluctant to concede he wasn't a "drug user."

The disclosure provisions can also be a two-edged sword, as I sadly found out when I checked out my own dossiers. To find out what one company had on me (only, it turned out, that I had a charge account), I first had to furnish them with: my name, social security number, current address, addresses for the last five years; and wife's name. Like many other inquiring consumers, I left with the distinct impression that if there hadn't been a dossier on me at the time I walked in, there was one after I walked out.

Fortunately, help may finally be on the way. "In the wake of some of the Watergate revelations, the whole privacy area is opening up," is how Congressman Edward I. Koch (D–N.Y.) put it.

ZINGING

As never before, Congress is examining private and governmental data collection, and some of the recent findings have horrified even perpetually blase legislators. In February, for example, four former employes of Retail Credit Company, the General Motors of the Credit Field—it reported by has reports on over 46 million Americans—told some narrowing stories:

Of derogatory information quotas that investigators were required to fill in order to keep their jobs. Of pressure to produce an inordinate amount of reports a day, "more than twice the amount that could be reasonably produced by a careful investigator," as Proxmire noted. Of "zinging," manufacturing, information on clients.

Of ruining the career of one bank exec because initial adverse allegations about his drinking and social habits were copied repeatedly—without verification—until he was fired as uninsurable.

Retail Credit denies the allegations. In January, however, the FTC took an unprecedented step—issuing a formal complaint against the firm alleging it "has used unfair or deceptive means in collecting and reporting information and in addition has violated the Fair Credit Reporting Act."

In light of Senate hearings and new Presidential interest, Proxmire believes there's now a 50–50 chance of a strengthened FCRA becoming law this year. His proposals would eliminate the fee most consumers now pay to see their records and generally allow them better redress for their grievances.

On another front, Sen. Sam Ervin (D–N.C.) has been holding hearings to limit the FBI's new centralized criminal data bank set-up, and Koch has introduced legislation to make governmental records available to each American along the lines of a recently enacted Swedish law.

ENCOURAGING

Perhaps the most encouraging development for individual privacy victims has been the opening up of the privacy field for litigation. For years, lawyers were reluctant to take on privacy cases because precedents were few and monetary rewards doubtful.

Even as new privacy legislation is introduced, modern technology comes up with new ways to subvert it. One expert notes that, very shortly, it will be technically feasible to store a 20-page dossier on each American on a piece of tape less than 5,000 feet long.

"Congress must act before these new systems are developed and before they produce further widespread abuses," notes Sen. Ervin.

"Stripped of our privacy, we lose our rights and privileges," concludes Ervin. "The Bill of Rights then becomes just so many words."

The stakes are high.

[From the Washington Star-News, May 25, 1974]

THE INFORMATION SEEKERS: YOUR PRIVACY IS THEIR CONCERN

(By John Fialka)

A new political issue, based on growing fears about the centralized use of personal information, is emerging in the wake of the Watergate scandal.

The issue involves the right of the American citizen to a certain degree of privacy, both from queries by governmental agencies and from the scrutiny of a large, but little known cluster of commercial agencies that make it their business to know about other people's business.

The extent of a person's right to privacy—a question that has languished for years in ill-defined, shadowy corners of the nation's legal system—will soon be given considerable attention by Congress and state legislatures.

Almost unlike any other issue today, privacy is enjoying enthusiastic, often passionate support from both the political left and arch-conservatives. Sometimes gatherings on the privacy issue can be mind-boggling to people used to seeing things in terms of conservatives battling liberals.

For example, in March the American Civil Liberties Union staged a month-long campaign on the right of privacy in New Mexico. The windup speaker for the ACLU—which is traditionally a supporter of left-wing causes—was Barry Goldwater, Jr., who sees the issue as being "right down the mainstream" of conservative thought.

Finding political support from both the right and the left, the White House recently announced that it will also launch an investigation into the privacy issue.

For the White House and the politicians now digging into the issue, the biggest assembler of data on the lives of ordinary, law-abiding people lives right under their noses, it is the federal government.

Nobody knows for sure how much data the federal government collects. A subcommittee of the Senate Judiciary Committee has spent four years studying the problem and will soon publish a 4,500 page description of the process which places the number of federal data banks at between 800 and 900. Some 54 different federal agencies are involved.

One might get some idea of the size of the federal operation by considering a proposal for a new nationwide computer system recently put forward by the General Services Administration.

It would involve about $100 million worth of new equipment that would replace 60 older computers now run by GSA or the Department of Agriculture.

One of the more excitable members of Congress, Rep. John E. Moss, D–Calif., has charged that the system would allow the government to assemble "dossiers on any individual or institution."

But Dennis Bracy, a GSA computer specialist says the public should not be alarmed. An elaborate system of "passwords" and code numbers will prevent people who are allowed in one section of the new system from getting into other parts of the system.

"We are not going to be able to know what's in Agriculture's computers and they are not going to know what is in ours," he added.

Despite the system's size, according to Bracy, it will amount to "about 1 percent of the government's computer capacity."

The question of how to control people who control data is one that has bothered some government officials since the computer hardware selling boom of the late 1960s left Washington awash in data systems.

Last summer, a panel of experts commissioned by the Department of Health, Education and Welfare to study the problem, concluded that computers have proved to be spectacular at solving some types of problem and are of little or no use in others.

Nevertheless, wherever they were installed, they were kept busy. "The successes were so spectacular," the HEW panel noted, "that the prestige of having a large-scale data processing capacity often prompted managers to keep the computers running, even at a financial loss."

Keeping computers running sometimes involves feeding them more data than they should have. For instance, the HEW study mentions the case of the National Driver Register, operated by the Department of Transportation, which is supposed to flag drivers with bad traffic records who attempt to get drivers licenses from more than one state.

Rather than going over their records to pick out the more flagrant violators, the states who contributed to the system found it easier and cheaper just to punch in all license applications.

The result, according to the study, was a kind of "dragnet effect," matching 5,000 applicants a day with records of traffic violations in other states. Because of the over abundance of data the matches were so imprecise that the 5,000 "hits" by the computer often had to be winnowed down to 500 by DOT staff.

The mismatch of data by one computer is a problem that could be catastrophically compounded if someone found a common language that could jump data out of dozens of different government data banks at once.

The HEW panel concluded that the "common language" already exists to a considerable extent in the use of an individual's Social Security number as an identifier for other purposes.

Originated as an easy way to keep track of survivor benefits and retirement pay under the Social Security Act in 1935, the idea of using the numbers for people spread like wildfire.

Today the federal government uses Social Security numbers to keep track of unrelated programs involving: aliens, Indians, soldiers, high school students, welfare cases, civil servants, taxpayers and people who buy or sell securities.

States use it on drivers licenses and many banks use it to identify accounts.

Because the willy-nilly use of the Social Security number would "enhance the likelihood of arbitrary or uncontrolled linkage of records about people," the HEW panel called for the government to stop using the number as a universal identifier and to develop safeguards to keep unauthorized persons from using it to penetrate government data banks.

These and other conclusions of the HEW report have been translated into legislation by Rep. Goldwater and Edward I. Koch, D–N.Y. It is pending before Congress.

The report, called "Records, Computers and the Rights of Citizens" is also being championed by the ACLU, which has accused HEW of continuing to expand the role of the Social Security number despite its report.

As far as the ACLU is concerned, the privacy issue might as well be called "Son of Watergate."

The ACLU's interest in privacy, according to Douglass Lea, head of the organization's privacy project, was considerably accelerated by the discovery of the "enemies lists" and other items among the evidentiary baggage associated with Watergate—including recent White House transcripts—that show the Nixon administration was aware of the potential damage a government might create by using its files on certain individuals.

The problem, the organization discovered, was that even with the example of Watergate, few people were aware of how large the public and private apparatus for tracking people's lives had really become.

"These things tend to come on cat's paws," asserts Lea who has been assembling a kind of glossary on what people can do if they know the right numbers.

A knowledgeable businessman, for instance, can tell from the code on certain credit cards whether a person pays his bill promptly.

The code on a veteran's discharge form can tell a knowledgeable employer whether the man had such problems as bed wetting or homosexuality, Lea discovered.

But businessmen do not have to depend on cracking government codes to find out about people's private lives. There are enormous private organizations who make their living doing that.

In theory, most of these are regulated by the Fair Credit Reporting Act, passed by Congress in 1970 to protect consumers against inaccurate or misleading credit reports.

Loopholes written into the law, however, still do not permit a consumer to see the results of a credit investigation done on him.

The problem has recently been aggravated by major oil companies who have been trying to get out of the credit card business and are looking for convenient reasons to deny further credit to card holders, according to Sheldon Feldman, assistant director for special status of the Federal Trade Commission which is charged with enforcing the law.

Once credit is denied, for whatever reason, the denial becomes part of the grist for credit reports that are bought and sold. Under the law, according to Feldman, a consumer is entitled to know which company's report on him results in a denial of credit.

Finding out why credit was denied, however, can be a big problem. "The law is fuzzy on that," says Feldman. "You can get them to look at your report and tell you what they think might be derogatory among the information in it. But you can't see it if they won't let you."

Opening a credit file would reveal, among other things, the company's system for grading credit risks, something that, according to Feldman, is "very jealously guarded."

Who does get to see credit reports? Almost any businessman who wants to buy one. Mike Wallace, the CBS news correspondent, once tested the system by printing up a letterhead for a nonexistent company and asking 20 credit bureaus for reports on various individuals. Ten responded with full reports without asking any questions.

Early this year, Gordon Forbes, a lawyer for the Minnesota Railroads Association, decided he needed to know more about Mrs. Betty Henry, a woman who has been campaigning for tougher state legislation on railroads.

He purchased a report on the woman from the Retail Credit Company, the nation's largest credit research firm. The incident caused a considerable flap in the Minnesota legislature, but Forbes could not understand why people were getting so excited.

"There was nothing secret about the ordering of the report," he noted in a news conference, "and it was done in accordance with my previous, routing requests in the handling of legal matters in my law practice."

How are reports prepared? The most extensive files on the average consumer are usually developed when he asks for life insurance. Somewhere in the dense thicket of words on the policy he signs is an authorization for the investigation.

Insurance companies want to know much more about an applicant besides how he pays his bills. Reports for insurance companies can involve checking neighbors to see if he drinks too much, has an unhappy home life, engages in dangerous sports or has any other life-shortening traits that would not endear him to insurance company actuaries.

In the trade, the Retail Credit Co. of Atlanta, Ga., is to insurance credit investigations what General Motors is to the automobile. Retail Credit says it has over 33,800,000 investigative reports on people.

Exactly how Retail Credit does its reporting is a matter of some controversy. Recently, several former company investigators told a Senate subcommittee that the company requires as many as 20 cases to be completed daily by one investigator and sets quotas for the production of derogatory material.

To meet the caseloads, the former employes said, they often had to use unverified records and sometimes even concocted information that went into the files.

Retail Credit has denied their charges. The company is also contesting charges by the FTC that company investigators use fraudulent means to obtain information and sometimes do not interview "sources" listed as having been interviewed.

Because the company is so big (it has 1,500 offices throughout the country) it is difficult to avoid dealing with Retail Credit. If you don't buy life insurance, you are likely to run into the company when you apply for credit from a local store.

Retail Credit has a subsidiary called Credit Bureau Inc. which has 80 offices, including one in Washington, that sell credit information to local businesses.

Thus, if you apply for a credit card, for instance, the business will turn around and get your history of paying your bills and records of related court problems from Credit Bureau Inc.

And even if you don't buy life insurance and don't ask for credit from anyone, you could still have Retail Credit looking into your life.

Mahlon A. Barash, of Arlington, Va., discovered this last summer when a woman who identified herself as a representative of "Welcome Neighbor" appeared on his doorstep.

Barash and his wife, Leah, were new in the Washington area and the woman gave them free gifts and told them about local churches, schools and stores. She also managed to ask them about their income, estimated expenditures, number of credit cards and occupations.

According to Barash, the woman did not tell them about Credit Bureau, Inc., until his wife spotted the company's name on a brochure, 20 minutes into the interview.

For Barash, the "welcome" to the Washington area was a troubling incident. "My wife would never have let her in if we knew who she was. I got pretty hot about it the more I thought about it."

For the FTC, Barash's complaint was an old story. The agency brought a cease and desist order against Credit Bureau, Inc. of Washington in 1971 after similar complaints. The order requires the hostesses to identify Credit Bureau, Inc. FTC lawyers are now investigating the new complaint.

According to James Perkins, assistant vice president for Credit Bureau's national operations, the agency is following the order to the letter.

The 25 Welcome Newcomer "hostesses" who work for Credit Bureau, Inc., in the Washington area are trained to identify themselves right away, he explains.

And if a person never asks for credit, according to Perkins, then the Welcome Newcomer service will not tell Credit Bureau, Inc., about him. And Credit Bureau, Inc., in turn, does not exchange information with the insurance files of the parent company, Retail Credit.

Company policy assures that "no files are mixed," Perkins explained to a reporter.

Although some of its methods may not be fully understood to the public, retail credit operates like the public library compared to another giant of the private investigation industry that is based on a computer system in Boston.

This is the Medical Information Bureau, known as the MIB to insurance men, who use the system to determine if there is any reason why an individual would not be a good medical risk for life insurance.

According to the executive director, Joseph C. Wilberding, the MIB has files on 11 million Americans and accumulates more than 2.2 million new files annually.

In most cases that data has come unwittingly from consumers who have agreed to permit a life insurance company to gain access to their medical records in order to buy life insurance.

Seven hundred insurance companies pool such information with MIB. If they have found evidence that the consumer has alcoholism, sexual deviation, psy-

chiatric problems, or a criminal record in his past history, that information is likely to go to the MIB.

Each type of problem is identified with a code number which member companies can use to query the MIB system.

The function of the MIB has proven to be fascinating to men like Sen. William Proxmire, D-Wis., who have been worrying about the privacy problem.

In Senate hearings last fall, Proxmire asked Wilberding if the Nixon administration could have saved itself the anguish of having to break into the office of Daniel Ellsberg's psychiatrist if it was familiar with the MIB.

"What could happen," theorized Proxmire, "is something like this. If the 'plumbers' had been a little more thoughtful, what they could have done was to get an insurance company to determine the psychiatric code numbers, and then they could have gone to the insurance companies . . . and on the basis of having gotten that information without having to rifle files or break in or go through all the ramifications that have caused such distress to the President of the United States."

Proxmire's idea was unsettling to Wilberding who protested that the MIB makes "spot checks" that would prevent such a query from happening.

"Who does the spot checking?" asked Proxmire.

"Our staff," replied Wilberding.

"How many people on the staff do you have doing that?" asked Proxmire.

"One, and we are expanding it," responded the MIB executive.

Besides expanding their one-man force that polices the system, MIB has done a number of other things after the encounter with Proxmire to make the public more aware of their operations.

Now, for the first time, according to the company, insurance applicants will be able to read about the MIB and its operations before they sign for insurance. Applicants may also ask the MIB to disclose information on their personal files.

But Proxmire intends to press for a law on the subject because under the current law the MIB is covered by a loophole that exempts medical data banks from federal regulation.

Despite the prospect of more federal law on the subject, people who yearn for the privacy of the "good old days" in the commercialized world of 1974 are dreaming.

"You can't function in this country and be left alone because you need things like life insurance and credit," asserts the FTC's Feldman.

And Feldman and other critics of the investigatory industry are quick to point out that cheap life insurance and cheap credit cannot exist without efficient systems to give companies enough data to make intelligent decisions on risks.

Thus, the tiny threads, the webs of information that mark our lives will still be collected.

Because the politics of privacy are running strong, however, Congress may soon make the consumer more aware of the process and set down a set of ground rules.

As for the "good old days," they really weren't that private. Most novels and plays of the bygone era of small town America show that the most intimate details of peoples' lives were often a staple currency for town gossips.

The difference is that people used to have a measure of control over those who felt the need to gather such data. You could see them, confront them, even punch them in the nose if their reports were wrong.

Those days are gone forever.

[From the Washington Star-News, June 15, 1974]

NEXT: THE CASHLESS SOCIETY (BUT WILL YOU LIKE IT?)

(By John Holusha)

A checkout clerk at the Hinky Dinky supermarket in Lincoln, Neb., is ringing up a load of groceries.

As he finishes, the shopper hands him a small plastic card. The clerk picks up a nearby telephone which is attached to a small keyboard terminal.

He dials a number. A soft, feminine voice comes on the line. "Proceed."

The clerk puts the card in the terminal and begins pressing buttons, which are arranged like those on a touch-tone telephone.

"Withdrawal request for one-zero-zero dollars, zero-zero cents," the voice says. "Proceed."

A few more keys are punched.

"Transaction completed."

The clerk has been talking to a computer. He has just withdrawn $100 from Lincoln's First Federal Savings and Loan Association so the shopper can pay for her groceries and have some cash for other purchases.

With a bit more button pushing he could have deposited a paycheck, automatically credited the price of the groceries to Hinky Dinky's account, held out some cash and put the remainder of the wages in the shopper's savings account.

This is the world of electronic funds transfer (EFT), loosely called the "cashless society."

It is the system that is going to free us from our old paper-bound ways of handling and spending money, its backers believe. They include computer companies, big bankers and major retailers.

Others have reservations. Consumer leaders and civil libertarians feel there are basic questions concerning privacy, security and consumer rights that must be answered before the nation rushes headlong from paper to electronic impulses.

But the trend is unmistakable. In San Francisco and Atlanta you can have your paycheck deposited directly in a bank and have the bank automatically deduct to pay fixed bills like mortgages and insurance.

In Upper Arlington, Ohio, when you shop at certain stores, the money shifts from your account to the stores' instantly.

Plans are afoot to develop a national electronic payments system.

Behind the movement is compelling economic necessity. The American Bankers Association says it costs $10 billion a year to process checks. And at the rate the usage of checks is increasing, they fear they'll be drowned in paper in a few years.

Retailers have never solved the problem of dealing with checks. They know they can't expect people to carry large amounts of cash, particularly in big cities. But a foolproof system to detect phony checks (an estimated $1 billion yearly) has yet to be devised. With electronic payment, the money is in their account at the moment of sale.

Makers of computers, terminals and all the other appurtenances of data processing see bulging order books for the rest of their days.

The Lincoln experiment, temporarily halted by protests from local banks that an S&L is poaching on their preserves, is only a small, tentative step toward the use of electronic money.

What the future may hold is to be demonstrated starting later this year in Pittsfield, Mass., a community of 77,000 nestled in the picturesque Berkshire hills. Pittsfield will become the first city in the nation where a family will be able to take care of virtually all its needs without using checks or more than pocket cash.

The system designed by a leading proponent of EFT, Dale Reistad of New York, will work like this:

Employers will send rolls of magnetic tape with payroll information to a computer center. The center will electronically direct the pay to employee accounts in any of the six banks, S&Ls or credit unions participating. The choice of institution is the employee's.

Then when he goes shopping, the emplove uses a plastic card. Each institution's card will have different markings but will "look" the same to the terminal. Virtually every store and service establishment in Pittsfield is to be in the system except for two big national chains, which have company policy problems, and bars and liquor stores, which weren't asked.

At first the system will be off-line. That is, records of purchases will be held until the end of the day and then run through the banks to adjust the balances. Eventually Reistad hopes it will go on-line, so the shift of funds takes place immediately.

The advantage to consumers is convenience and the fact that checking accounts can pay interest in Massachusetts. Being spared long sessions trying to balance a checkbook will also be a relief to some.

A different sort of inducement is offered by a big savings bank in Wilmington, Del.: A 2 percent discount on everything but food.

It's offered by the Wilmington Savings Fund Society and is called the WSFS (pronounced whizz-fizz) Plan. It involves an interest-bearing savings account, a free checking account and the WSFS card.

A person buying something with the WSFS card at any of 1,200 locations that accept it in Delaware signs what looks like a standard credit card form. Actually, it is the equivalent of a check.

At the end of the day merchants send the slips to WSFS, which switches the money from the customer's account to the store's.

Once a month, the WSFS computer adds up all the purchases made with the card, calculates 2 percent of that and puts it into the customer's savings account. It sends a bill for the 2 percent to the merchants.

The consumer gets 2 percent off. The merchant doesn't worry about bad checks. WSFS avoids having to process tons of paper.

The only place the system doesn't work is in food stores which have profit margins under 2 percent. Giving the discount would put them out of business.

WSFS devised the 2-percent-off plan as a means of attracting cutomers. Most EFT experts agree that a lot of bait will be needed to hook consumers nationally into a checkless system.

"How do you get the customer to switch from a system he is basically not unhappy with?" a banker asked at a recent symposium.

With instant payments, the customer loses the "float." Float refers to the time it takes a check to get back to the bank it was written on for payment. Writing a check and rushing to the bank the next day to cover it is an elementary way of "playing the float."

Float is even more important with credit cards. Bank cards like Master Charge can give the user up to two months' float—in effect a free loan.

It often takes as long as four weeks for card charges to be tabulated and sent out as a bill. Most cards have another four-week grace period before interest charges begin. By waiting until near the end of the grace period to write a check, a consumer uses the money free.

There are more deeply felt causes of consumer hostility. A study conducted by the Booz, Allen & Hamilton consulting firm documented what many have suspected: Most people fear and dislike computers.

"The fear of being 'lost' or 'trapped' by an arbitrary machine is crystallized for many consumers in the image of the computer," the study noted. "Indeed, it is difficult to adequately emphasize the intensity of negative feelings which consumers express toward automation and computerization."

The study included sample comments from persons interviewed about their attitudes toward computers. Among them was this classic:

"This discussion of computers reminds me of something that happened to me. I was in this gas station and a fellow came up and put a quarter in the Coke machine and nothing came out. He really wanted a soda so he dug in his pocket for two dimes. Nothing came out. He didn't even get a nickel back. So he took out the biggest gun I've ever seen in my life and shot it five times. Honest to God, I just got a warm feeling. It felt good. The machine was totally destroyed. He had a contented look on his face."

Beyond the emotional reaction are real issues of who will control a person's finances, himself or a bank? If the whole system is electronic how will a person who has overextended himself a bit delay payment on some bills to meet more pressing obligations?

What will he do if a mistake is made somewhere? This involves an individual's entire financial structure, not just one bill. How do you argue with a computer?

EFT apostles advise adding an ombudsman to the system and downplaying the part computers play. "Sell financial services, not computers," says Reistad.

So far the systems haven't sold well. Response to the pre-authorized payment experiments in California and Atlanta has been "slow," a recent banker's meeting was told. An experiment in Seattle under which a person could pay his bills, figure his budget and do advance tax calculations using a touch-tone phone collapsed for lack of interest.

Another consumer option that would be lost is the ability to stop payment on a check after a sale. University of Southern California law professor Edward Dauer pointed out in a letter to the Federal Reserve Board that the power to stop payment "gives the drawer the ability to force a conversation about the underlying transaction."

With the money in the seller's coffers, the consumer's only recourse is through the courts against a vastly more powerful foe.

Security is another problem. Since the Equity Funding case, in which computers were used to falsify records involving millions of dollars, the public is suddenly aware of "computer crime."

What is to prevent a clever, computer-trained crook from tapping into a system and with a few impulses transferring millions from other accounts to his?

Even if they can be tracked down, can they be prosecuted? Criminal laws were written in the days when outlaws actually took the money and ran. The laws didn't envision misdirected electrical impulses.

An attorney for Seattle-First National Bank said it is unclear whether the criminal statutes of Washington state apply to "criminal activities involving computers and paperless transactions."

On the personal level, what happens if a consumer loses the card he uses for purchases? It's not like losing a credit card; with an EFT card unauthorized use will mean money actually taken from the owner's account.

Automatic cash dispensers have already been installed by several area banks, including National Bank of Washington, First National Bank and Union Trust in the District and Maryland National across the D.C. line.

These cash dispensers are designed to help blunt the argument that direct pay deposit will leave people constantly strapped for small amounts of cash.

The current security approach is for the user to memorize a number for use with the card. In some automatic cash dispensers, the machne takes the card in through a slot and waits for the number to be punched on a keyboard. If the wrong number is keyed in it spits out the card. Three or four wrong tries and it swallows the card.

This system depends largely on the magnetic code strip on the card. At a recent conference on card security, the head of a systems company pointed out that the stripe encoding can be easily duplicated.

One avenue being investigated is tying the card to some unalterable physical attribute of the user. Research is centering on fingerprints, voiceprints, hand geometry and signature analysis.

Another kind of security, the right of an individual to feel secure in the privacy of his transactions, is threatened by EFT, just as it has been in every area where computers have made it possible to store and retrieve vast mountains of information.

Responding to the Federal Reserve Board's request for comments on a nationwide electronic payments systems for banks, Robert E. Smith of the American Civil Liberties Union pointed out that the Treasury can order copies of all a person's checks, deposit stubs and other records kept for government inspection.

With a paper system it is not practical to do this, but with electronic storage a person's entire financial history will be available "at the touch of a button," Smith said. The very existence of such a system "will make unauthorized access to such data more likely."

Ironically, the comments received by the Fed show that those who know computers best are the most concerned about invasion of privacy.

"Will other agencies have access to this data: FBI, IRS, state and local revenue enforcement agencies and police?" a former official of the Association for Systems Management wrote.

An executive of a computer company, Control Data, was more blunt. "A checkless/cashless situation is in effect a seizure of personal papers" and a violation of the Fourth Amendment to the Constitution, Charles Eumurian declared.

(The Fourth Amendment states that "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated. . . .")

The ACLU pressed for tough rules in any EFT system restricting access to financial information as well as to the money itself.

The Fed's initiative may well have the effect of hastening the restructuring of the nation's financial system.

At present banks are allowed to have checking accounts, thrift institutions like savings and loans are not. There are numerous exceptions, but that is the general rule.

In return, the thrifts are allowed to pay more interest to attract deposits and have some tax advantages.

The thrifts and commercial banks have engaged in a running controversy over who has the unfair advantage, each trying to obtain the other's prerogatives.

The proposals for electronic transfer has provided new things to fight over.

The major banks are lobbying to have S&Ls excluded from any national payments system. Let the S&Ls do business with their neighborhood bank, they say.

The S&Ls complain that such an arrangement would dry up their source of funds and cripple the housing industry, which they largely finance.

The banks, in turn, say if S&Ls can participate in EFT they will have the equivalent of checking accounts. This was the argument brought against First Federal in Lincoln.

Congress has had under study for several months legislative recommendations based on a lengthy study that would blur the distinctions between the different types of banking. More recently, a two-year, $2 million study of EFT has been proposed by Sen. Thomas J. McIntyre, D-N.H.

Since the political clout of both the bankers and S&L associations on Capitol Hill is considerable, it is unlikely an electronic system that harms either fundamentally will be approved.

More likey is some kind of simultaneous progress on banking reform and EFT.

EFT enthusiast Reistad flatly predicts the development of a national banking system.

What then is the future for electronic money and the consumer?

A Reistad aide predicts that by 1980, 70 percent of the nation's 625 large retailers will have installed point-of-sale terminals. (Several large Washington stores, including Woodward & Lothrop, already have done so.)

Simultaneously, automated clearing houses to electronically settle accounts between banks in certain areas will have been established.

The advantages—to the retailers and bankers—of tying the store and banking systems together are already being discussed at high-level meetings. It would give stores access to customer accounts no matter where they choose to bank in an area.

A national EFT system would permit the same kind of transaction anywhere in the country—possibly not instantly, but faster than paper.

A large percentage of paychecks, particularly government checks, will be directly deposited.

And there probably will be a lot of plastic in our wallets.

Reistad's Payment Systems Newsletter quotes the former president of the company which licenses Master Charge cards, Harold Hassinger:

"In the not too distant future all of an individual's credit needs will be handled under a line or lines accessed by his card. The same card will also give him access to his checking or savings account not only via the automatic cash dispensing machine . . . but at the merchant's terminal at point of sale.

"In fact," Hassinger goes on, "some of the more imaginative bankers believe that ultimately there will be a total financial service for the individual including his demand deposit and time cash balances, his debt balances—both short and long-term—both secured and unsecured, and his investments, all accessible through the card and all recorded on a combined statement showing his total financial condition."

[From the New York Times, Sept. 30, 1973]

Use of Personal-Characterization Coding on Military Discharges Is Assailed

(By Peter Kihss)

On one veteran's DD 214 form, the record of his Army discharge "under honorable conditions," was the code "SPN" followed by a number. He wondered about it after a public utility here asked to see the form and then turned him down for a job.

The number meant a discharge for "disloyal or subversive security program," according to William Pankratius, military justice associate for the Workers Defense League of 150 Fifth Avenue, a 37-year-old human-rights and legal-defense group.

"I asked him if he had any idea why he had gotten it," Mr. Pankratius related. "He said he had received antiwar literature in the mail. But he said 'the hell with it'—he'd get another job elsewhere."

The league says it has obtained a current list of 530 code listings for SPN's—the "separation program number designators" maintained by the Defense Department for the armed services.

CATEGORIES ARE BROAD

The group said this was a list revised as of last Nov. 1 and still in effect despite controversies over the last two years. Mr. Pankratius asserted that "virtually every large corporation in America has had access" to at least earlier versions of the codes.

The numbers affixed to any kind of discharge from honorable to dishonorable cover such routine classifications as "expiration of term of service" or "dependency" or "hardship."

But they also include such broad tags as "marginal producer," "unsuitability—apathy, defective attitudes and inability to expend effort constructively—individual evaluation" (meaning one superior's view), "importance to national health, safety or interest," "interest of national security," "convenience of the Government, other reasons, or as specified by Secretary of the Army" and even only "other good and sufficient reasons."

OTHERS ARE LISTED

Characterizations may be more specific, as "unfitness—unsanitary habits," "sexual deviate," "homosexual acts," "habits or traits of character manifested by sexual perversion," "unsuitable—enuresis—board action" (referring to an administrative board) which involves bed-wetting, "theft," "indebtedness—failure to pay," "nonsupport of dependents" and "early release of Puerto Rican personnel who failed to qualify for training," which may involve language problems.

In Washington, Defense Department spokesmen said that SPN codes had been restricted to "For Official Use Only" for more than a year and that the entire procedure was "under review."

The department declined to provide a list of SPN's or to confirm the Workers Defense League's set. But the spokesmen said a new list of designators had been developed reducing the number from 530 to 126, with present plans to put this into effect not earlier than next July 1.

RESTRICTIONS PLANNED

Twenty-five members of the House of Representatives, led by Edward I. Koch, Democrat-Liberal of Manhattan, and Lee Aspin, Democrat of Wisconsin, have cosponsored bills to bar any statement on discharge certificates as to why a serviceman was released.

The bills would also prohibit the military from making the information available to any private person or entity other than the veteran concerned. Further, they would permit veterans already holding discharge certificates with some designators to get new certificates omitting the information.

Representative Koch has decried what he called "unfortunately common knowledge as to what the code numbers designate" and "invasion of privacy which may never end for a veteran with a prejudicial SPN."

M'GOVERN BILL FILED

He said the same code number had been usd to identify a discharge for heroin addiction or for simply smoking marijuana. Mr. Koch asserted that there had been "rank injustices" and that "surely thousands of people who are suffering silently as a result of Defense Department policy" aside from complaints that have been made.

A Senate bill has been introduced by George McGovern, Democrat of South Dakota.

The SPN system dates back to about 1947. As late as spring, 1972, separate sets of each service's designators were available in open publications of Army, Navy, Air Force and Marine Corps regulations.

Melvin R. Laird, when he was Secretary of Defense, ordered a study started in March, 1972, after Senator Harold E. Hughes, Democrat of Iowa, asserted during an inquiry into drug abuses that Pentagon computers could "spit out a number that could destroy" a veteran in civilian life. The study has not been completed.

PROTECTION IS CITED

Defense Department spokesmen said the numbers were for internal use by governmental agencies, with the original DD 214 form going to the veteran, copies to his branch of military service and to Selective Service for records and

estimation of future availability, and one copy to the Veterans Administration for its use in dealing with benefits.

The reason for the number system, they said, is "to protect an individual against invasion of privacy." They cited a regulation that said, "military services will not, in absence of written authorization from the former member, furnish a copy of the form or any information to nongovernmental organizations or individuals."

"Prospective employers or others," the regulation continues, "are required to obtain this information from the separated member."

The defense officials said that the DD 214 form must be signed by the serviceman at the time of his discharge, and that he would be told on request what was the reason for the SPN code. The reason could be decided anywhere along the line, from his immediate commanding officer to a court martial.

A former serviceman, the spokesmen said, may apply for correction at any time within 15 years after his discharge. Each military service has a review board which may change a discharge—aside from court-martial cases—"to correct an inaccuracy or to cure an injustice," they said.

Barbara Downey, assistant to Representative Koch, said a Defense Department report showed 725,740 servicemen discharged in the year ended last June 30—653,838 with honorable, 39,120 with general, 29,442 with undesirable, 2,906 with bad conduct and 434 with dishonorable discharges. Even an honorable discharge can include a bad SPN designator, she said.

[From the Washington Post, Sept. 12, 1973]

LIVING BY THE NUMBERS

To those who fear the day when machines will know all too much about men, the social security number has become an object of concern. That nine-digit number has advantages. It distinguishes one person from everyone else with a similar name, and thus can serve to keep the records straight. But what makes the social security number so helpful also gives it its ominous possibilities. Some fear that it could become the key which opens the way to computerized master files on individuals, and that a very personal identifier, very widely used, could bring about the surrender of personal control over the details of one's identity.

Such thoughts were stirred up by the news that the District of Columbia has just joined 10 states in using the social security number as the permit number for drivers' licenses. The District's new policy will not change the nature of its drivers' license files or open the way to the collection of any more information on District drivers, or make data available more widely than before. Its major direct impact, in fact, will be on those prospective drivers who do not have a social security card to show, for they will have to apply for a number, and endure a wait of several weeks, before their permit applications can be processed.

Even so, the District's action does illustrate what a Health, Education and Welfare Department advisory panel on computers and citizens' rights recently called "the drift toward" using the social security number as a universal identifier. The panel found that federal agencies, more than any other force, have fostered broader use of social security numbers over the years, all in the interests of efficiency. In the case of drivers' licenses this is certainly true. In the highway safety act of 1966, Congress directed the Department of Transportation to suggest uniform safety and driver training standards for the states. By the time this general mandate had been translated into bureaucratic manuals, there was a specific provision that the social security number would be useful as one way to tell one driver from another. The same rationale prompted the government to start using the number to identify taxpayers in 1961. That move has done more than any other single step to promote use of the same number for bank accounts, welfare records and a flock of other public and private records and accounts.

The real danger is that each additional use makes additional uses easier to justify and harder to avoid, until only the imperfections of computers—rather than the principles of people—will prevent the amassing of master files. In other words, the nation could be sliding toward the day of dossiers without ever having made a conscious decision to march in that direction. The HEW advisory committee found this alarming and called for prompt congressional action to limit the uses of the social security number and "establish safeguards providing legal sanctions against abuses" of personal records. The committee's specific proposals for safeguards deserve close attention on Capitol Hill. In the case of drivers'

licenses and other files, it may be highly desirable for the government to have other people's numbers. But such decisions should be made by legislators in full awareness of the broad issues involved.

[From the New York Times, June 28, 1970]

FEDERAL COMPUTERS AMASS FILES ON SUSPECT CITIZENS—MANY AMONG HUNDREDS OF THOUSANDS LISTED HAVE NO CRIMINAL RECORDS—CRITICS SEE INVASION OF PRIVACY

(By Ben A. Franklin)

WASHINGTON, June 27.—The police, security and military intelligence agencies of the Federal Government are quietly compiling a mass of computerized and microfilmed files here on hundreds of thousands of law abiding yet suspect Americans.

With the justification that a revolutionary age of assassination, violent political dissent and civil disorder requires it. The Government is building an army of instantly retrievable information on "persons of interest."

The phrase is an agent's term for those citizens, many with no criminal records, whom the Government wants to keep track of in an effort to avert subversion, rioting and violence or harm to the nation's leaders.

Critics of this surveillance, so far few in number, believe that the collection and dissemination of such information on noncriminals—for whatever purpose—is unauthorized by law and raises the most serious constitutional questions.

The foremost among them, Senator Sam J. Ervin, Jr., Democrat of North Carolina, has said that computerized files already in existence here are leading the country toward a "police state."

Discussions with officials, an examination of some known data files and information supplied by the Senate show that the files often contain seemingly localized and mundane information, reflecting events that today are virtually commonplace.

The leader of a Negro protest against welfare regulations in St. Louis, for example, is the subject of a teletyped "spot report" to Washington shared by as many as half a dozen Government intelligence gathering groups.

The name of a college professor who finds himself unwittingly, even innocently, arrested for disorderly conduct in a police roundup at a peace rally in San Francisco goes into the data file.

A student fight in an Alabama high school is recorded—if it is interracial.

Government officials insist that the information is needed and is handled discretely to protect the innocent, the minor offender and the repentant.

The critics—including the Washington chapter of the American Civil Liberties Union and Representative Cornelius E. Gallagher, Democrat of New Jersey—charge that the system is an invasion of privacy and a potential infringement of First Amendment rights of free speech and assembly.

MASS SURVEILLANCE SYSTEMS

Senator Ervin, a conservative, a student of the Constitution, a former judge of the North Carolina Superior Court, and the chairman of the Senate Subcommittee on Constitutional Rights, says that the advent of computer technology in Government file keeping is pushing the country toward "a mass surveillance system unprecedented in American history."

In a recent series of Senate speeches, Mr. Ervin said that the danger was being masked by a failure of Americans to understand "the computer mystique" and by the undoubted sincerity and desire for "efficiency" of the data bank operations and planners.

The Government is gathering information on its citizens at the following places:

A Secret Service computer, one of the newest and most sophisticated in Government. In its memory the names and dossiers of activists, "malcontents," persistent seekers of redress, and those who would "embarrass" the President or other Government leaders are filed with those of potential assassins and persons convicted of "threats against the President."

A data bank compiled by the Justice Department's civil disturbance group. It produces a weekly printout of national tension points on racial, class and political

issues and the individuals and groups involved in them. Intelligence on peace rallies, welfare protests and the like provide the "data base" against which the computer measures the mood of the nation and the militancy of its citizens. Judgments are made; subjects are listed as "radical" or "moderate."

A huge file of microfilmed intelligence reports, clippings and other materials on civilian activity maintained by the Army's Counterintelligence Analysis Division in Alexandria, Va. Its purpose s to help prepare deployment estimates for troop commands on alert to response to civil disturbances in 25 American cities. Army intelligence was ordered earlier this year to destroy a larger data bank and to stop assigning agents to "penetrate" peace groups and civil rights officials of the Army say they "assume" they are not.

anizations. But complaints persist that both are being continued. Civilian Computer files intended to catch criminal suspects—the oldest and most advanced type with the longest success record—maintained by the Federal Bureau of Investigation's National Crime Information Center and recently installed by the Customs Bureau. The crime information center's computer provides 40,000 instant, automatic teletype printouts each day on wanted persons and stolen property 49 states and Canada and it also "talks" to 24 other computers operated by state and local police departments for themselves and a total of 2,500 police jurisdictions. The center says its information is all "from the public record," based on local and Federal warrants and complaints, but the sum product is available only to the police.

A growing number of data banks on other kinds of human behavior, including, for example, a cumulative computer file on 300,000 children of migrant farm workers is kept by the Department of Health, Education, and Welfare. The object is to speed the distribution of their scholastic records, including such teacher judgments as "negative attitude," to school districts with large itinerant student enrollments. There is no statuory control over distribution of the data by its local recipients—to prospective employers, for example.

WARNING BY ERVIN

Senator Ervin has warned: "Regardless of the purpose, regardless of the confidentiality, regardless of the harm to any one individual [that might occur if there were no computer files], the very existence of Government files on how people exercise First Amendment rights, how they think, speak, assemble and act in lawful pursuits, is a form of official psychological coercion to keep silent and to refrain from acting."

But despite his sounding of such alarms, Senator Ervin has noted that there is "unusual public and Congressional complacency." When he speaks on the Senate floor of "techniques for monitoring our opinions" and of "grave threats to our freedoms," the chamber is more often than not nearly empty. He has gained little Congressional support and scant attention outside the Congress.

Meanwhile, various official and high-level pressures on Government agencies to acquire computers and to advance their surveillance are producing results.

The pressures include a stern recommendation for the broadest possible surveillance of "malcontents" and potential assassins by the Warren Commission, which investigated the assasination of President Kennedy. The commission's mandate is widely cited in the Government as the authority for citizen surveillance.

The commission, headed by former Chief Justice Earl Warren, disapproved as too narrow, the criteria for persons to be brought under "protective" surveillance proposed in 1964 by the Secret Service. The guidelines were "unduly restrictive," the commission of "some manifestation of animus" by disgruntled and activist citizens before those persons could be brought under Secret Service surveillance as potential "threats to the President."

EVERY AVAILABLE RESOURCE

"It will require every available resource of the Government to devise a practical system which has any reasonable possibility of revealing such malcontents," commission said.

The guideline was broadened. A computer was installed by the Secret Service last January. The commission's edict became a surveillance bench mark.

For surveillance of persons who may be involved in civil disturbances, the riots of 1967 and 1968 served the same purpose.

"The Warren Commission and the riots legitimized procedures which, I grant you, would have been unthinkable, and frankly, unattainable from Congress in

a different climate," one official said. "There are obvious questions and dangers in what we are doing but I think events have shown it is legitimate," the official declined to be quoted by name.

Senator Ervin contends that in the "total recall," the performance, the speed and the interconnection of Government data files there "rests a potential for control and intimidation that is alien to our form of Government and foreign to a society of free men." The integration of data banks, mixing criminal with noncriminal files, is already underway, according to his subcommittee.

INTEGRATION OF FILES

The subcommittee has been advised by the Department of Housing and Urban Development, for example, that its data systems planner's have proposed to integrate on computer tape files concerning the following: the identities of 325,000 Federal Housing Administration loan applicants; the agency's own "adverse information file," the Justice Department's organized crime and rackets file, and F.B.I. computer data on "investigations of housing matters." The object, the Department said, is a unified data bank listing persons who may be ineligible to do business with HUD.

As another example of how computer data proliferates, the subcommittee cites a report it received from the Internal Revenue Service.

The I.R.S., with millions of tax returns to process, was one of the earliest agencies to computerize. It has also had a reputation as a bastion of discretion. The privacy of individual tax returns has been widely regarded as inviolate, to be overcome only by order of the President.

But the subcommittee has been told that the I.R.S. has "for many years" been selling the state tax departments—for $75 a reel—copies of magnetic tapes containing encoded personal income tax information. It is used to catch non-filers and evaders of state taxes.

The District of Columbia and 30 states bought copies of the I.R.S. computer/covering returns from their jurisdictions in 1969, the service has told the subcommittee. Each local jurisdiction was merely "requested" to alert its employees that the unauthorized disclosure of Federal tax data was punishable by a $1,000 fine.

FIREARMS DATA FOR SALE

The I.R.S. also sells at cost—apparently to anyone who asks—the copies of its data files of registrants under the various Federal firearms laws it enforces.

The Secret Service computer file is capable of instant, highly sophisticated sorting and retrieval of individuals by name, alias, locale, method of operation, affiliation, and even by physical appearance.

The agency's Honeywell 2200, with random access capability, makes it possible to detect, investigate and detain in advance "persons of interest" who might intend—or officials concede "they might not but we don't take chances"—to harass, harm or "embarrass" officials under its protection.

Unknown to most Americans, the name, movements, organizations and "characteristics" of tens of thousands of them—criminals and noncriminals—are being encoded in the Secret Service data center here.

The names of other thousands have been inserted in less specialized computers operated by the Justice Department and the F.B.I. Although the agencies insist that they do not, the computers can—and Senator Ervin stresses that no law says they may not—"talk" to each other, trading and comparing in seconds data that may then spread further across the nation.

The Secret Service can now query its computer and quickly be forewarned that, say, three of the 100 invited guests at a Presidential gathering in the White House Rose Garden are "persons of protective interest."

Under current Secret Service criteria, they may have been regarded by someone as the authors of reportedly angry or threatening or "embarrassing" statements about the President or the Government. The action taken by the Secret Service may range from special observation during "proximity to the President" to withdrawal of the invitation.

What constitutes a computer-worthy "threat" thus becomes important. The Secret Service asserts that it applies relatively easy-going and "sophisticated" standards in deciding who is to be encoded. But the critics point out that the vast capacity of computer for names and dossiers—unlike that of a paper filing system, which has self-limiting ceiling based on the ability to retrieve—is an encouragement to growth.

The information or "data base" for a Secret Service computer name check flows into the protective intelligence division from many sources—abusive or threatening letters or telephone calls received at the White House, F.B.I. reports, military intelligence, the Central Intelligence Agency, local police departments, the Internal Revenue Service, Federal building guards, individual informants.

Much of it that may be "of interest" to the Federal monitors of civil disturbance data is screened out, Secret Service spokesman say, or is merely name-indexed by the computer with a reference to data reproducible elsewhere.

According to guidelines distributed by the Secret Service last August, the types of information solicited for insertion in the computer—broadened at the insistence of the Warren Commission—included items about:

Those who would "physically harm or embarrass" the President or other high Government officials.

Anyone who "insists" upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.

Those who may qualify as "professional gate crashers."

Participants in "anti-American or anti-U.S. Government demonstrations in the United States or overseas."

In an interview, Thomas J. Kelley, assistant director of the Secret Service for protective intelligence, said the computer name insertions already totaled more than 50,000. The Secret Service is extremely careful, he said, both in evaluating the encoded subjects and in checking to determine that those who receive a print-out are entitled to it.

But there apparently is no formal guideline or list of criteria for dissemination, as there is for insertion. And direct, automatic, teletype access to the computer from the distant Secret Service bureaus—the system used by the airlines and the National Crime Information Center—may be the next step, Mr. Kelley said.

Nothing demonstrates how remote access multiplies the output of a computer better than the crime information center's system staged by the F.B.I. in 1966.

With direct-access teletype terminals in 21 state capitals and large cities, the information center computer here can be queried directly by local police departments on the names, aliases, Social Security numbers, license tag numbers and a broad array of stolen goods (including boats) that come hourly before the police.

An officer in a patrol car tailing a suspicious car can radio his dispatcher, ask for a check of a license number, and be told by teletype and radio in less than a minute that the automobile is stolen and that its occupants may be "armed and dangerous."

With one of the newest and most sophisticated random access computers in Federal service the Secret Service data center can also perform some wizardry that no other equipment here can master. It can be ordered, for example, to print out a list of all potential trouble makers—"persons of protective interest"—at the site of a forthcoming Presidential visit. The random access scanning can be geographical.

Photographs and descriptions can be assembled for the traveling White House detail. Investigations, even detentions, can be arranged at the site.

"You take a waiter in a hotel dining room where the boss is going to speak," a Secret Service spokesman explained. "Let's say the computer turns up his name and we investigate and decide it would be better for him to be assigned to some other duties. No one has a constitutional right to wait on the President, you know. That's how it works."

Cued by another more elegant electronic program, the same computer can also produce all the information it contains on the "characteristics" of subjects encoded on its tapes—all the short, fat, long-haired, young white campus activists in Knoxville, Tenn., for example. Only the Secret Service computer can do that.

The American Civil Liberties Union office here protested last October that the Constitution protects such acts as an effort merely to "embarrass" a Government official, the persistence of citizens in seeking redress even of "imaginary" grievances, and their participation in "anti-U.S. Government demonstrations." The Secret Service, however, has declined to withdraw or amend its intelligence reporting guidelines.

"They seem satisfactory to us," Mr. Kelley said. "If we weren't getting the information we want, we'd change them."

Under the heading, "Protective Information," the guidelines read as follows:

"A. Information pertaining to a threat, plan or attempt by an individual, a group, or an organization to physically harm or embarrass the persons protected by the U.S. Secret Service, or any other high U.S. Government official at home or abroad.

"B. Information pertaining to individuals, groups, or organizations who have plotted, attempted, or carried out assassinations of senior officials of domestic or foreign governments.

"C. Information concerning the use of bodily harm or assassination as a political weapon. This should include training and techniques used to carry out the act.

"D. Information on persons who insist upon personally contacting high Government officials for the purpose of redress of imaginary grievances, etc.

"E. Information on any person who makes oral or written statements about high Government officials in the following categories: (1) threatening statements; (2) irrational statements, and (3) abusive statements.

"F. Information on professional gate crashers.

"G. Information pertaining to 'terrorist' bombings.

"H. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war.

"I. Information regarding anti-American or anti-U.S. Government demonstrations in the United States or overseas.

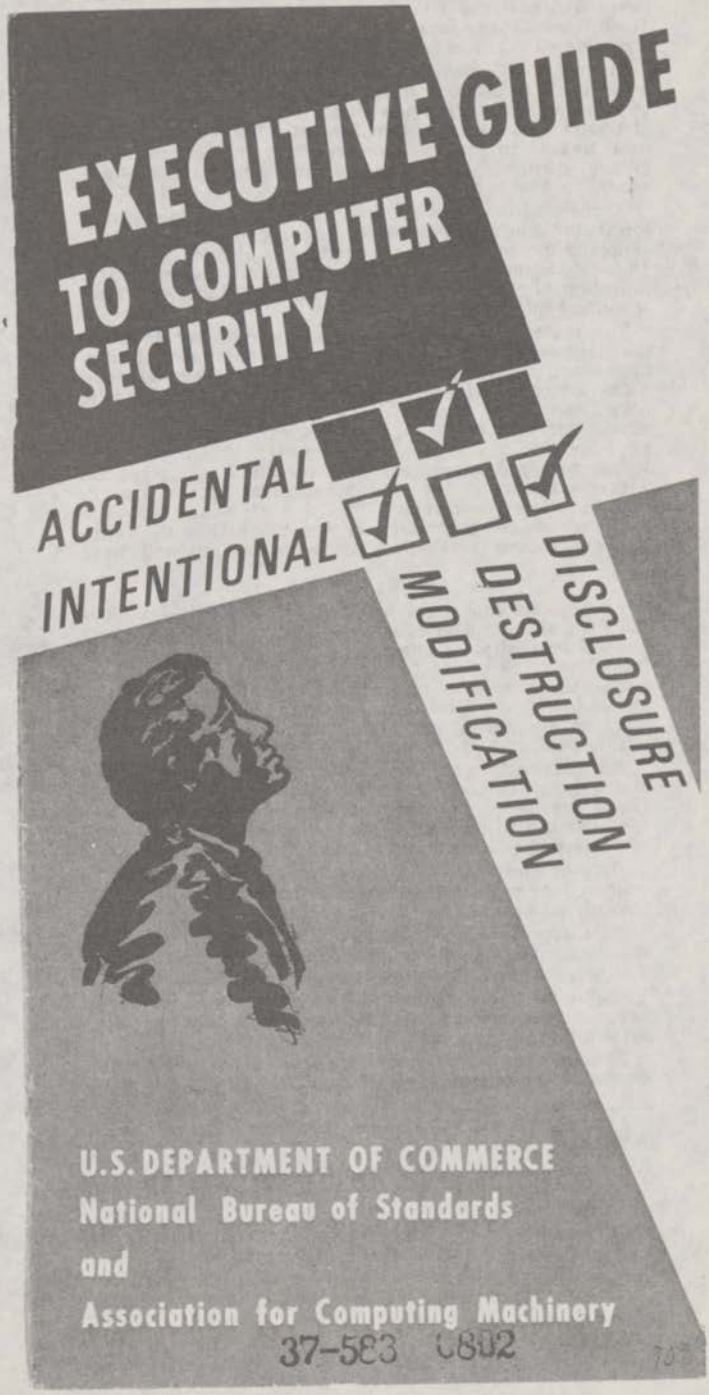
"J. Information regarding civil disturbances."

Senator Ervin, who is noted for a piquant sense of humor, said in a speech a few months ago: "Although I am not a 'professional gate crasher,' I am a 'malcontent' on many issues.

"I have written the President and other high officials complaining of grievances that some may consider 'imaginary.' And on occasion I may also have 'embarrassed' high Government officials."

Based on the guidelines, the Senator asserted, he himself is qualified for the computer.

PUBLICATIONS OF THE NATIONAL
BUREAU OF STANDARDS



37-583 0802

FOREWORD

This booklet has been prepared for an audience of executives and managers, other than computer and ADP managers, in organizations using computers to help them understand the necessity for computer security and the problems encountered in providing for it.

There are still many gaps in our knowledge. Much more work needs to be done before an organization will be able to implement security provisions which are specific and justifiable responses to defined threats. There are, however, measures which may be taken and this booklet provides a general discussion of those solutions which are available today.

A question and answer format was selected to organize the material in a manner which might logically represent a general approach to analyzing computer security problems. The material in this booklet was drawn from the report of a workshop of top technical experts in the field of computer security, held in December 1972.

The Institute for Computer Sciences and Technology at the National Bureau of Standards, U.S. Department of Commerce and the Association for Computing Machinery, the nation's largest technical society for computer professionals, have been jointly sponsoring* a series of workshops and action conferences on national issues. These workshops were designed to bring together the best talents in the country in the respective areas to establish a consensus on 1) current state of the art, 2) additional action required, and 3) where the responsibility for such action lies. The workshop on computer security was the first in the series and did, indeed, establish a precedent of satisfying those goals.

BASIC TERMS

Privacy is a concept which applies to an individual. It is the right of an individual to decide what information about himself he wishes to share with others and also what information he is willing to accept from others. The privacy issue has not resulted from the development of computers, but the heightened interest in it can be laid to the capability of computers for storing vast amounts of readily usable data.

Confidentiality is a concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection which will be provided.

Data integrity exists when data does not differ from its source documents and has not been accidentally or maliciously altered, disclosed or destroyed.

Data security is the protection of data against accidental or intentional destruction, disclosure or modification, using both physical security measures and controlled accessibility.

Controlled accessibility is the set of technological measures of hardware and software available in a computer system for the protection of data.

Physical security is protection against physical destruction and theft of assets, including data.

---

* The National Science Foundation provided financial assistance in planning the series.

WHY SECURITY?

1. WHAT IS COMPUTER SECURITY?

Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs and data to assure that organizational assets and individual privacy are protected.

2. WHY SHOULD I CARE ABOUT COMPUTER SECURITY?

Computer data and programs represent an increasingly important part of the assets of every organization in our economy. Every day both business and government become more dependent on computer systems to carry out normal business operations. There are over 130,000 computers installed in the U.S. today representing a current value of $29.2 billion. There is no way to place a value on the millions of data files and programs used on these machines, or on the value of the services performed by these same machines. Their worth in this sense is clearly inestimable. These assets must be safeguarded.

Consumer and public interest groups as well as individuals are now beginning to demand that their concern for protection of individual privacy be taken into account in the design and operation of modern information systems. The President in his 1974 State of the Union address called for attention to this critical national problem at the highest levels of government. His concerns included modern information systems, data banks, credit records, and electronic snooping as well as ostensibly collecting personal data for one purpose and then using it for another. In fact a number of bills are currently being proposed in the states as well as the Federal legislatures to insure rights of privacy and establish requirements of data protection. Every data processing activity will be impacted by the provisions of the legislation.

Every organization will need to adopt procedures and provide safeguards to protect these valuable assets and meet the requirements of legislation.

3. WHAT MUST I PROTECT THESE ASSETS AND INFORMATION AGAINST?

Threats to computer system security arise from the unpredictability of environmental conditions and people. Data processing facilities and assets must be protected against natural catastrophe and hostile activity so that the impact on the operations of the organization are minimized. These threats include destruction by environmental forces as well as theft or destruction by individuals. Nature only destroys; man both destroys and acquires. Exposure to these threats creates risk for your organization.

4. ARE THE THREATS WHICH CAN BE PERPETRATED BY PEOPLE ON MY COMPUTER SYSTEM REALLY SERIOUS?

Such threats are very *real* and *serious*. Companies have been nearly put out of business by unauthorized manipulation of their data files.

The most common situation is the manipulation of computer system resources for personal gain. Direct physical assaults on computer facilities for purposes of destruction are relatively rare. Nevertheless persons motivated by revenge or antipathy toward modern technology have made direct physical assaults resulting in serious damage.

In a study of computer-related crimes, the significant fact appeared that many people who consider themselves honest citizens who would not steal from other people have no compunction about stealing from a computer because it is a faceless nonentity. The same study revealed that the financial gain from computer crime has little appeal for some people, but they will commit a crime for the thrill of "beating the computer".

In reading the following examples, it will be obvious that the individuals involved were apprehended, but it must be assumed that much computer-related crime is not detected and is, in fact, still going on.

a. Internal threat, job related: Because of his familiarity with a bank's programs and procedures, a teller in a New York bank was able to transfer $1.5 million to his own account without leaving any trace of his activity, completely foiling both

automated and manual auditing systems. Authorities became suspicious only when his name was associated with a large betting operation.

b. Internal threat, not job related: An EDP manager and part of his staff used their company computer to "handicap" horse races and pocketed the profits.

c. External threat, computer manipulation: An engineering student discovered a way to gain access to the computerized supply system of a telephone company. He claims to have obtained and sold nearly $1 million in equipment before getting caught.

d. External threat, forms manipulation: A man substituted deposit slips, magnetically coded with his account number, for the blank ones available on a bank's customer counter, causing the computer to place other customers' deposits in his account. He then withdrew the money and disappeared.

SITUATION TODAY
(The Real World)

5. ARE THE MAIN PERSONNEL THREATS TO A COMPUTER SYSTEM WITHIN OR OUTSIDE AN ORGANIZATION?

Without question, the "trusted insider" is the greater threat to any computer system. An employee (programmer, janitor, or even manager) with knowledge of the system and its defenses is the most likely to subvert a system. The inept ones are caught immediately; the competent ones may go undetected indefinitely. As organizations place more and more valuable data into large data banks, the potential payoff for an inside job will get bigger and bigger.

6. CAN DATA IN A COMPUTER SYSTEM BE COMPLETELY PROTECTED?

No. For every defense there is an alternative offense, but a level of security can be provided that is commensurate with the risk. The desired protec-

tion level is that which makes the cost of subverting the system greater than the benefit to be gained by its subversion.

7. CAN STORED DATA BE SECURE FROM DESTRUCTION OR COMPROMISE?

Security of stored data depends on the storage media and the threats to which they are vulnerable. There are two types of threats:

—individuals who have physical access to the storage media.

—individuals who have computer access to the storage media.

In the first case, experiments have demonstrated that magnets can destroy data stored on magnetic media, but must be placed in almost direct contact with the medium, e.g. magnetic tape, to cause damage. Physical access to the storage area must therefore be carefully controlled.

In the second case, a user of a computer system can erase data on storage media (either accidentally or maliciously), using the computer. The attack which is most difficult to detect comes from someone who deliberately and surreptitiously modifies stored data for his own benefit.

8. CAN COMMERCIAL COMPUTER SERVICES BE EXPECTED TO PROTECT DATA?

To a limited degree and for a price. Computer services usually operate insofar as possible according to guidelines and instructions provided by their customers; special care such as the use of a dedicated computer may be provided for users if requested and paid for. Eventually, the requirement for computer security may create specialized computer facilities which are certified to be secure for specified purposes.

9. IS A DEDICATED SYSTEM SECURE?

A system dedicated to a specific task is more secure than one in which the tasks are still being developed or are rapidly changing. Reservation systems in which the terminal operation has only limited data entry/retrieval capabilities are difficult to probe.

The security of such systems depends on careful control of the actions the user may perform; however, the integrity of data in these systems still depends on the integrity of the source.

10. WHY DON'T COMPUTER MANUFACTURERS "BUILD-IN" PROTECTIVE DEVICES AND OFFER TOTAL SECURITY PACKAGES?

Until recently there has not been a general requirement to develop protected computer systems. Hardware and software solutions have not been found for all security problems. However, some protective devices, such as automatic equipment for personal identification, will become available, or perhaps even "standard", just as automatic transmissions did in the auto industry. Toward this end, large groups of users with similar security needs, such as the Federal Government, can lead the way by establishing uniform specifications of security for computer systems.

11. DO SPECIFICATIONS EXIST FOR A SECURE COMPUTER FACILITY?

No specifications exist for a general computer system to achieve a given level of security. Dedicated systems have been implemented to specifications based on restricted security requirements using restrictive solutions. General security solutions may be found for some common problems, but each facility must define its own detailed specifications.

12. ONCE I HAVE DETERMINED REQUIREMENTS FOR MY FACILITY, HOW CAN I ASSURE THAT THEY ARE SATISFIED?

Through compliancy testing. Security features are usually evaluated for completeness, effectiveness, and correctness. Then they are subjected to simulated attempts to breach security. For example, if a security feature of a system is the authentication of remote terminal users through randomly generated passwords which are periodically replaced, then a compliancy test would be a check to see if any of a specified number of randomly generated fake passwords would be accepted. Good design specifications include the range of compliance which will constitute an acceptable test.

13. CAN COMPUTER SECURITY AND THREATS TO THAT SECURITY BE MEASURED?

Computer security can be measured in terms of the probability that a facility's defenses will be breached by specific threats. For example, the operating system of a secure computer must be designed so that the probability of a penetrator obtaining executive control of the computer system—and thus access to all programs and data—is extremely low. No theoretical methods exist for assigning numerical probabilities to such a situation occurring in the various types of computer systems. Only when a large body of statistics has been accumulated for specific threats can honest numbers be assigned as probabilities. Until then measurement of computer security and the threats to it will be based primarily on intuition and limited experience.

VULNERABILITIES

14. WHAT IS THE MOST VULNERABLE POINT IN ANY COMPUTER SYSTEM?

Relatively speaking, remote terminals are the least secure points of computer system. A system is more vulnerable if it may be accessed from remote terminals both because of the possibility of "bugging" and because remote terminals typically have little supervision. A remote terminal provides a convenient spot from which a would-be penerator could launch a software attack. This is an attack on a system in which the penetrator gains entry either by simulating another's identity or by using anomolies of the system to probe the hardware and software defenses in order to access unauthorized data or to obtain control of the executive programs. Such an attempt could be disguised as a parametric study of efficiency or other "system" study involving a wide range of hardware and software. Once he finds the key to executive control, the penetrator can compromise any data he wishes and can also erase evidence of his attack and leave a way open for future access.

15. CAN A SHARED SYSTEM BE SECURE?

Shared systems are currently not secure because of their complexity and lack of cohesive security

design. Computers can be shared in several ways with varying degrees of security. In order of increasing risk, some examples of computer system sharing are:

—Batch-processing systems which sequentially process users' programs while sharing the central processor between a single user and the input/output system. A user of this system has little control in obtaining others' data while it is being processed but may obtain it while it is being prepared for processing, either accidentially or intentionally, through his program.

—Multi-programming systems processing several *local* users' programs simultaneously. A user can accidentially access another users' data, but the central processor will not be under his direct control, eliminating most opportunities for deliberate compromise of data.

—Multi-programming systems allowing programs and data to be entered remotely. Such systems are vulnerable to the same threats as a local multi-programming system as well as to threats associated with remote terminals.

—Interactive time-sharing systems processing several users' programs simultaneously. Each user has interactive control over his program and can therefore actively search for other users' data. Some time-sharing systems also allow remote access and consequently are subject to threats through remote terminals.

16. CAN COMMUNICATION LINES BETWEEN COMPUTERS OR BETWEEN COMPUTERS AND PERIPHERAL EQUIPMENT BE BUGGED?

Assuming that "bugging" means the surreptitious attachment of "listening" devices to computer equipment, the answer is, "Yes". The communication lines linking a computer facility with peripheral equipment in other buildings, with remote terminals, and with other computers in a network are highly vulnerable to electronic eavesdropping.

17. IS BUGGING THE ONLY FORM OF ELECTRONIC EAVESDROPPING?

No. Electromagnetic and acoustic emanations from a computer facility can be detected and interpreted

by a listening post outside but in the vicinity of the computer center. However, detecting these emanations is not "bugging" since a listening device need not be attached to equipment or planted within the computer facility. Communication lines, unshielded electromechanical equipment, and CRT terminals can act as signal sources. All such emanations must be suppressed to achieve a highly secure environment.

18. IT SEEMS THAT AT PRESENT NO COMPUTER SYSTEM IS SECURE. IF THAT IS TRUE, WHAT CAN I DO?

Although a system which has been designed without security as a prime objective cannot be totally secure, much can be done to improve its security. Systems designed for security are under study now. In the interim, the actions available for improving security fall into two main classes: technical and management solutions.

TECHNICAL SOLUTIONS

19. WHAT ARE THE TECHNICAL SOLUTIONS?

They fall into three categories of solutions: computer-based protection techniques, identification techniques, and security audit techniques. All three must be integrated into a secure system according to its security requirements.

20. WHAT ARE COMPUTER-BASED PROTECTION TECHNIQUES?

They are methods based either on hardware or software, but are in either case an integral part of the computer system design, which perform functions such as keeping the data files of different users segregated in a shared system. Some of these techniques are available now such as memory read/write inhibit and segmentation of primary and secondary storage. New programming techniques also permit a compartmentalized approach to data handling.

In systems of the future designed with security as a primary consideration, access to processing resources and data files will be centrally controlled

37-583 O - 74 - pt. 2 - 45

and restricted to a minimum. Design will be based on modular structure in which every module will be like a watertight compartment in a ship; access to one module will not automatically permit access to any others. The barriers between users will be well defined to limit accidental damage and inhibit browsing through another user's files or programs. In addition, technical design criteria for secure systems will include requirements for access controls to be active at all times with no possibility for manual bypassing and for security features to be specified in terms of complete design, correct implementation and proper installation and operation. Data in communication links will be protected, e.g. encrypted.

21. BUT WHAT CAN BE DONE NOW?

In addition to the memory segregation and programming techniques mentioned above, data can be encrypted during both transmission and storage. Encryption, also known as scrambling, is the most inexpensive way of protecting data travelling over long distances from electronic eavesdropping. It is also effective for data in storage or in memory in a shared system. However, it is a method of protection especially subject to internal subversion; its success depends on the security of periodically changed keys. The keys are only as secure as those who have knowledge of them.

22. HOW CAN DATA INTEGRITY BE DETERMINED AND MAINTAINED?

Data integrity may be verified by checking the data or its representation against something known to be accurate. At one extreme, this means checking it word for word against its source. If the source is on tape or in some other machine readable form, the checking can be done by computer, but it is still expensive and time-consuming.

Problems may also be discovered by analyzing systematic errors, trends, and error frequency, but more popular is the use of error-detecting bits, which produce error "flags" when the sums of the data being used do not check with the equivalent sums in the original data. "Bounds controls" are useful because they can sound a warning when data items

37-583 O - 74 - pt. 2 - 47

are not within certain limits, e.g. an inordinately large check is being issued by a payroll program. Data integrity can also be maintained through redundancy, either by having duplicate copies of the data or by processing the same job on different machines.

23. WHAT ARE THE IDENTIFICATION TECHNIQUES?

Identification is simply the recognition of an individual, a program or a set of data from a name or identification code. Authentication is the verification of identity—a double check, so to speak. Authentication may require that the user supply his unique password or enter his unique key-card. Authentication may even involve physical verification of the claimed identity.

24. HOW DOES A COMPUTER SYSTEM AUTOMATICALLY AND RELIABLY VERIFY LEGITIMATE USERS?

A computer system can verify a legitimate user in three ways:

a. From his knowledge of a password, phrase, number, or other privileged information. Passwords are widely used today. They are, however, rather easily obtained by unauthorized persons either from those knowing them or from their notes and printouts, or even directly from the computer memory.

b. From his possession of a unique physical key, such as a card containing unique information. Such physical items, however, are easily lost, stolen, or counterfeited.

c. From automatically measured biometric data, such as hand geometry, fingerprints, voiceprints, etc. These biometric methods promise high reliability and accuracy, but most techniques are still in the research stage.

25. WHAT IS MEANT BY SECURITY "AUDIT"?

Computer system auditing involves an independent and objective analysis of the security of a computer system. A security audit determines the adequacy and effectiveness of system controls vis-a-vis their threats. It includes both scheduled evaluations and after-the-fact investigations of attempted penetrations of the computer system. An automated, real-time audit mechanism can often provide a timely alert of penetration attempts. Whether after-the-fact or real-time, the auditing procedures should provide

sufficient information for damage assessment and for purposes of prosecution.

26. WHAT IS AN "AUDIT TRAIL"?

An audit trail is a record of what processing is being done to specific data and programs in the system and by whom. To be useful this record should be organized (preferably automatically) into reports of the following types:

—Alerts of possible security violations.
—Review of system activity.
—System security status summaries.
—Damage assessment reports.

27. WHO SHOULD DO THE AUDITING?

Both internal and external auditors should be employed. Both should audit some of the same systems so that results can be compared directly. It is important that internal auditors occupy a neutral position as high in management as possible, i.e. they should not have any responsibility for ADP operations.

MANAGEMENT SOLUTIONS

28. WHAT ARE SOME MANAGEMENT SOLUTIONS?

Planning, funding and implementing security solutions are fundamental management actions. In particular, the areas to be considered include physical security planning, personnel selection and education, system selection and procurement of computer system security options, security certification and provisions for computer operations security. Controls used to achieve computer security must be uniformly enforced because of the value of the commodities and assets being protected; this is the reason for total management involvement.

29. WHAT ARE SPECIFIC MANAGEMENT STEPS THAT CAN BE APPLIED TO IMPROVE COMPUTER SECURITY PLANNING?

First, appoint an independent manager of computer system security, i.e. other than the ADP operations managers, with direct authority in security matters. Then organize a computer security program

and conduct a risk analysis. The security program should make provisions for:

—Specifying precisely who can read, use, or modify data. Ensure that technical as well as administrative controls are used to implement these instructions.
—Conducting independent internal and external audits.
—Keeping accurate and up-to-date organization charts, delineations of responsibilities, and work statement.
—Maintaining and promulgating thorough and detailed plans for normal operations, emergency operations, and recovery operations.
—Motivating employees to report insecure practices or suspicious activities, as well as to maintain their own security awareness.

30. WHAT KINDS OF PHYSICAL PROTECTION SHOULD BE CONSIDERED FOR A COMPUTER FACILITY?

The first line of defense consists of good engineering management:

—Locate in areas not exposed to floods, wind, high tides, fire, etc.
—Construct a facility which can be easily guarded.
—Ensure that electromagnetic emanations are minimized.
—Install emergency power sources, water pumps, air-conditioning, etc.
—Provide adequate emergency maintenance facilities.
—Operate the facility to ensure personnel safety.
—Provide backup for data and for data processing.

31. WHAT PERSONNEL SELECTION PROCEDURES ARE NECESSARY BEYOND NORMAL HIRING PRACTICES?

Perhaps none if present practices include a comparison of the candidates' previous salary with his present standard of living and personal wealth (or debts) and careful verification of previous employment records, character references and reasons for leaving.

32. WHAT EDUCATIONAL PROGRAMS ARE NEEDED IN SECURITY?

Security education and training should not be a one-time thing. Refresher courses and periodic security reviews should be required for all personnel. In addition to the basic indoctrination, the following should be considered:

—Handbooks with security rules and penalties for their violation fully and clearly specified.

—Educational and motivational posters.
—Dissemination of some (but obviously not all) of the security measures in force at your facility.
—Publicity for selected cases of computer abuse at other installations when the penalties imposed were severe. Details of perpetration should be omitted, however.

33. WHAT IS SECURITY "CERTIFICATION"?

Certification is a managerial declaration that the security features of a computer system comply with the specifications which, in turn, satisfy the security requirements. The details of technical analysis leading to security certification are not well specified at this time and there is no certifying agency, as such. However, some prerequisite actions necessary to this process are:

—Modeling of the system and the analysis of the model.
—Formalization of the access controls.
—Prediction of system security degradation and its effect.

Certification should take place at discrete points during the design, implementation, and operation of a system, viz.

—To check that the design is complete.
—To confirm that the implementation is correct.
—To determine that the installation meets all design standards and requirements.
—To establish that a system is secure after system modification, failure or penetration (either detected or suspected).

34. WHAT STEPS SHOULD BE TAKEN AFTER A PENETRATION IS DETECTED?

The status of the system's security must be analyzed to determine which portions have been affected and what has been lost. The unaffected portions may then be restarted, but it is crucial not to overlook any program modifications the penetrator may have left behind which permit easy re-entry at a later time. An important factor in computer system recovery is the existence of a reference point. A reference point is a backup set of key programs and data bases—certified to be correct and unmodified—stored at another secure location. With such a reference point and using operations logs and files, the step-by-step recovery and recertification of other programs and data bases can begin. Care should be taken that the access point through which penetration occurred is fully covered in the restored system.

35. WHAT ARE THE COSTS OF PROVIDING COMPUTER SECURITY?

The costs of providing computer security may be broken into three areas: initial cost, operational cost, and overhead cost. The importance of information processing in the business and governmental communities makes the assumption of these costs mandatory at a level commensurate with the risks to the system. At a minimum, this risk is equivalent to the value of the computer equipment.

Initial costs include:

—Physical security equipment controlling personnel access to the ADP facilities.
—Physical security equipment protecting data in storage.
—Additional equipment for identification, data encryption, program isolation, and security auditing.
—Operating system modifications and additional software needed to utilize this equipment.

Operational costs include:

—Salaries of security personnel.
—Maintenance of security equipment.
—Creating and updating user authorization lists, data file descriptions, data encryption keys, and data access records.
—Security training for operations personnel.
—Certifying and auditing system security.

Overhead costs include:

—Impact on computer system efficiency and flexibility.
—Impact on personnel attitudes.

36. WHAT BENEFITS MAY BE DERIVED FROM COMPUTER SECURITY?

The costs incurred in providing computer security must be placed in perspective to the benefits gained by providing it. These benefits include:

—Protection of individual privacy by compliance with security requirements of Federal and state legislation, management policy, and user confidentiality agreements.
—Protection of the physical assets of the computer facility.
—Protection of the financial investment in programs and data.
—Protection of the assets represented by data.
—Better system and data integrity.
—Better reliability and timeliness of data processing.
—Better accounting of data and resource usage.
—Better employee awareness of their importance to the organization.

SUMMARY

37. WHAT PRIORITY SHOULD BE ACCORDED THE VARIOUS MEASURES SUGGESTED FOR IMPROVING COMPUTER SECURITY?

The first step in computer security is simply controlling personnel access to the computer facility. Creating and maintaining a "security environment" will let both employees and outsiders know that safeguards exist.

Next come some administrative measures:

—List hardware and software resources (including data bases) in order of value.
—Perform a risk analysis.
—Formulate the goals of the security program.
—Determine the investment required to counter the estimated threats.
—Create a security organization, assigning it full responsibility for security.
—Plan a security program and implement it.

The order of priority for the next steps depends upon the cost/benefit studies. A common pattern might be:

—Upgrade the initial physical security measures.
—Establish personal identification systems and other controlled-accessibility procedures.
—Control the flow of data throughout the processes of collection, entry, storage, processing and dissemination.
—Make individual users personally accountable for control of, and access to, data.
—Implement software security to the degree indicated by the cost—benefit analysis.
—Shield the facility against electromagnetic leakage.

SUGGESTED READING

Davis, Ruth M., "Privacy and Security in Computer Systems: An Overview", CBEMA Privacy Series 2, Computer and Business Equipment Manufacturers Association, Washington, D.C., February 1974, 21 p.

Geller, Sydney B., "The Effects of Magnetic Fields on Magnetic Storage Media Used in Computers," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 735, July 1972, 30 p.

Parker, Donn B., Susan Nycum and S. Stephen Oüra, "Computer Abuse," Stanford Research Institute, Menlo Park, California, 1973, 131 p.

"Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems." U.S. Department of Health, Education and Welfare, Washington, D.C., July 1973, 346 p.

Reed, Susan K. and Dennis K. Branstad, "Controlled Accessibility Workshop Report," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 827, May 1974, 82 p.

Reed, Susan K. and Martha M. Gray, "Controlled Accessibility Bibliography," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 780, June 1973, 11 p.

Renninger, Clark R. and Dennis K. Branstad, "Government Looks at Privacy and Security in Computer Systems," U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., NBS Technical Note 809, February 1974, 37 p.

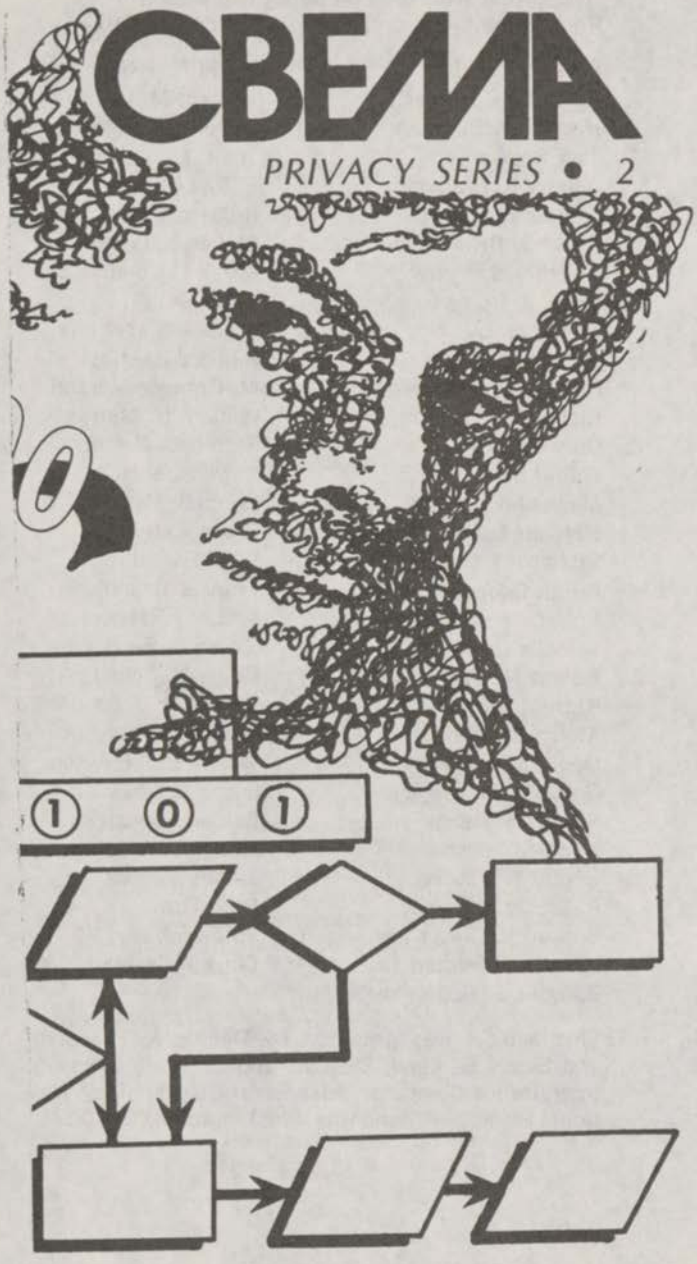
PARTICIPANTS

NBS/ACM Workshop on Controlled Accessibility
Rancho Santa Fe, California December, 1972

Robert P. Abbott
Alfred L. Basinger
Harvey W. Bingham
Joel Birnbaum
Dennis K. Branstad
William F. Brown
Peter S. Browne
G. Edward Bryan
Donal J. Burns
James H. Burrows
Jeffrey P. Buzen
Howard H. Campaigne
Richard G. Canning
Gary Carlson
Walter M. Carlson
Michael A. Casteel
Hatcher E. Chalkley
Richard W. Conway
Ruffin Cooper
Robert H. Courtney, Jr.
Isabelle Crawford
Robert M. Daly
Ruth M. Davis
Albert S. Dean, Jr.
Daniel L. Edwards
Philip H. Enslow, Jr.
Robert S. Fabry
Hilda C. Faust
Gerald W. Findley
R. Stockton Gaines
Edward L. Glaser
Lance J. Hoffman
Douglas L. Hogan
David K. Hsiao
William M. Inglis
S. Jeffery
John D. Joyce
E. Rex Krueger
Richard Leibler
Steven B. Lipner
Ralph L. London
Peter G. Lykos
Clair G. Maple
Richard G. Mills
M. Granger Morgan
William H. Murray
Eldred C. Nelson
A. Michael Noll
Donn B. Parker
Bruce Peters
C. J. Purcell
Francis J. Quirk
Anthony Ralston
Susan K. Reed
Roger R. Schell
Robert H. Scott
Kenneth C. Sevcik
Walter E. Simonson
Irving L. Solomon
Selden Stewart
Douglas W. Tompson
James Tippett
Rein Turn
Frederick Way, III
Clark Weissman

This booklet was prepared by Dennis K. Branstad and Susan K. Reed, Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

[GOVERNMENT LOOKS AT PRIVACY AND SECURITY AND COMPUTER SYSTEMS]



On November 19 and 20, 1973 the National Bureau of Standards (NBS) of the U.S. Department of Commerce sponsored a Conference entitled "Government Looks at: Privacy and Security in Computer Systems". The purpose of this conference was to review the issues and problems facing all levels of Government which are attempting to serve society in general while protecting the privacy of the individual citizen.

As part of a continuing program to encourage thought and discussion of the "Role of Computers in Privacy, Confidentiality and Data Security", the Computer and Business Equipment Manufacturers Association (CBEMA) has reprinted the conference speech by Dr. Ruth M. Davis, Director of the NBS Institute of Computer Sciences and Technology. CBEMA believes that Dr. Davis has presented a balanced, well-considered view of this complex subject from the Government point of view.

We applaud the initiative of the NBS in bringing together representatives of Federal, State, and Local Government, Industry and independent authorities to begin to seek nationally applicable solutions to the problems which have been raised.

Peter F. McCloskey
President

FOREWORD

The multi-dimensional nature of the Security in Automation problem defies easy or prompt resolution. Progress depends upon a proper understanding of the component parts of the problem and their interrelationships, and upon the recognition and assumption of relevant responsibilities by appropriate segments of the public and private sectors. My conference speech represents an attempt to stimulate thought, dialogue and action toward these objectives. I am pleased that CBEMA is taking this means to bring my views to the attention of a wide audience of concerned organizations and individuals.

Ruth M. Davis, Ph.D.
Director, Institute for
Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce

THE PROBLEM

There is a societal problem today that signals a major confrontation between the individual in modern society and modern technology. It is the problem variously referred to as that of "Invasion of Individual Privacy," "Data Security," "Computer Crime" or "Computer Security."

As a problem it may perhaps be a singular occurence or, on the other hand, it may be a tell-tale of the future in which the interaction between people and technology will become much more personalized and intense.

Certainly, the problem area which encompasses the privacy of individuals, the confidentiality of data and the security of computer systems is highly explosive and could, if not dealt with properly, trigger off negative chain-reactions as well as possibly damaging restrictive controls on many applications of technology.

At the same time, if the problem is treated lightly by the executive, judicial or legislative branches, if industry does not carry out its obligations to the public and if the scientific community disassociates itself from the technological underpinnings of the problem, then computer and communications technology could indeed victimize individuals and intrude upon their rights as citizens and consumers.

It is of little use to the public to simply highlight the vastness and complexity of the problem which will be described as the problem of "Security in Automation." What is needed is a sufficient understanding of the problem to describe its component parts, to assign responsibilities and to recognize a satisfying solution when it is presented.

COMPONENTS OF THE PROBLEM

The problem of "Security in Automation" is multi-dimensional in scope. Its several components can be characterized along the axes of:

Protection of the privacy of the individual: a responsibility of the judiciary and legislative branches.

Management of information in automated record-keeping systems: a responsibility of management and information management technologists.

Assessment and assignment of the costs of Security in Automation: a responsibility of the service industries and government.

Establishment of procedures, guidelines and standards to assure information management is in compliance with legislative and judicial requirements for privacy: a responsibility of government, management, industry and the public.

Development and application of the needed automation and information management technologies and products: a responsibility of industry, information services and the government.

Resolution of the problem of Security in Automation will result from the derivation of solutions that will satisfy all the individual problem components. It is an empty exercise to pass legislation that is technologically impossible to implement. Similarly, it is just a technological tour-de-force to design equipment or procedures that are too costly to use.

Progress towards resolving the problems of Security in Automation is thus dependent upon coordinated, in-step efforts of the judiciary, Congressional and state legislatures, Federal, state and local government management, information service industries and the automation and information technology industries.

Successful resolution of the problem also depends upon an understanding of the difference between its very important separable aspects of privacy, confidentiality and security.

PRIVACY APPLIES TO INDIVIDUALS

It is the right of an individual to decide what information about himself he wishes to share with others and also what information he is willing to accept from others; i.e., he is freed from observation by others when he is free to select from the universe the information he wishes to assimilate unto himself. This concept is in direct conflict with the present trend toward collecting and storing a large amount of information about everyone and then using it for a number of different purposes. The resolution of such matters will have to be achieved through legal channels and is not within the purview of controlled accessibility. The privacy issue has not resulted from the development of computers, but the heightened interest in it can be laid to the capability of computers for storing vast amounts of readily usable data.

CONFIDENTIALITY APPLIES TO DATA

It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection which will be provided. It is the confidentiality of data that requires protection, not the *privacy*.

SECURITY IS PROTECTION OF HARDWARE, SOFTWARE AND DATA

Security comprises:

Data security is the protection of data against accidental or intentional destruction, disclosure or modification using both physical security measures and controlled accessibility.

Physical security, as it pertains to computers, does not differ from physical security for other installations. It is achieved through the use of locks, guards, badges, personnel security clearances and administratively controlled measures outside the computer as well as measures required for the protection of the structures housing the computer and related equipment against damage from accident, fire and environmental hazard, thus ensuring the protection of their contents.

Controlled accessibility is the set of technological measures of hardware and software available in a computer system for the protection of data.

PRIVACY OF THE INDIVIDUAL

The issue of individual privacy is no more a modern phenomena than is record-keeping. Both are as old as society itself. They have, however, become of far greater concern to individuals and government as 1) computer technology has made record-keeping more effective and thus more widely employed, 2) service industries — both public and private — have become more dependent upon records about individuals for success in their operation and 3) the public has demanded more accountability by government and public enterprises.

As a result, the principal concerns about individual privacy today center around:

- The desire of the individual to exercise control over the collection of information about himself, and
- The desires of the individual to exercise some measure of control over the use of information about himself once it is collected.

THE JUDICIAL PROCESS AND INDIVIDUAL PRIVACY

The judicial system in this country provides protection to the individual and his rights. It is the judicial process which must address and interpret the law concerned with the rights of the individual to privacy. The Constitution of the United States and court-precedent law are primary sources for this protection. So also is Congressional and state legislation.

Although the Supreme Court has not accorded the right to privacy the status of a Constitutional right, it has recognized elements of this right. In a landmark case involving a state statute restricting the use of birth control, Justice Douglas, writing for the Court found the right of privacy to be implicit in rights afforded by the first, third, fourth and fifth amendments to the Constitution. In a more recent case, the Court indicated that a person may have the protection of due process, the right to a fair hearing and appeal to a higher authority with regard to the circulation of information about him.

LEGISLATIVE ACTIONS AND INDIVIDUAL PRIVACY

One of the most significant legislative actions, while not directly aimed at protecting individual privacy, has been the Fair Credit Reporting Act of 1970. This Act among its provisions, gives the individual the right to be informed of what information is maintained about him by a credit bureau or investigatory reporting agency. Items which are challenged as inaccurate by the person about whom the information is maintained must be reinvestigated by the maintainer of the file and corrected. If after reinvestigation the dispute is not settled, the agency must include a brief statement from the subject describing the dispute. While the enactment of this statute has been the most significant Federal action, state and local governments have also

been active in this area. The city of Wichita Falls, Texas has enacted an ordinance designed to protect computerized personal data, and the National Association of State Information Systems (NASIS) has been active in seeking to formulate model legislation in this area.

On September 5, 1973 a bill was introduced into Congress entitled "Code of Fair Information Practices of 1973." The intent of the Bill is to establish a Code of Fair Information Practice for automated data systems. The Code defines fair information practice as adherence to specified safeguard requirements, prohibits violation of the requirement, provides for civil liability and criminal sanctions against violators and provides temporary or permanent injunctions to stop violations.

In 1973, some seventy bills concerned with protection of individual privacy were pending in the fifty state legislatures. Passage of any significant number of these bills along with passage of some of the bills introduced into Congress could easily result in an unacceptable morass of conflicting requirements on service industries, technology and regulatory or judicial organizations. Some national coherence must exist for any realism to be present in arriving at security in automation adequate to protect individual privacy.

Legislative and judicial activity then is intense and increasing in its goal of providing adequate protection to the individual by allowing him measures of control over information about him which is collected and used through the medium of automated record-keeping systems.

THE PROCESS OF INFORMATION MANAGEMENT

Information management is an essential component of the generalized management process which occurs in all organizational units of society. This has always been so. In recent decades, however — particularly since the 1950's — there has been an increased concern with and an increased emphasis on information management.

The principal factors leading to the new emphasis on information management are identifiable. First of all, in the 1950's the United States transitioned from an industrial nation to post-industrial nation.[1] It was the first nation to so do with over half of its labor forces concentrated in the service industries. The change to a

post-industrial nation was not just a theoretical "paper-change." It meant, in practical terms, that success for organizations was dependent upon the proper use of information as the basis for control in their complex action mechanisms and intricate organizational structures.

This is in contradistinction to pre-industrial and industrial societies, societal stages through which the United States has progressed in becoming a post-industrial society or service economy. Success in pre-industrial societies is based on management of energy and production processes: but success in post-industrial societies is based on the management of information resources.

Information management is just one component of the management process. To try to make it inseparable from management in its entirety is to hinder progress in both information management and the generalized process of management.

Information management is a process which involves the many operations performed *on* information to accomplish a predetermined objective. It is helpful *not* to include the uses of information or decisions *about* its substantive content in information management. These latter type steps are better incorporated in other steps of the management process supported by other technologies and disciplines than that of information management.

To illustrate the extent of information management, it begins once the step is completed of deciding what information is desired for the management process in question. It does not include the use of the information by managers or the actions taken as a result of the information presented.

Information management does include the operations of:

1. Data collection,
2. Data validation,
3. Information processing or information handling,
4. Data transformation,
5. Record-keeping,
6. Information control including the operations associated with:
   Freedom of information
   Confidentiality of information
   Integrity of information
7. Information display and presentation, and
8. Standardization of information management operations.

The adequate performance of information management as thus described is an integral and essential part of the entire management process.

37-583 O - 74 - pt. 2 - 48

"SECURITY" AS A COMPONENT OF INFORMATION MANAGEMENT

The problems of data confidentiality and computer security cannot be dealt with in the abstract or out of context with the other components of the information management process. There are, for example, two other current public concerns which directly affect other aspects of information management. These coupled with the concern with security form a potentially conflicting triad of public concern over confidentiality of information, freedom of information, and integrity of information.

Actions undertaken to meet public concerns with protection of individual privacy must not run counter to these other demands on information handling currently being made. Guarantees of freedom of information already have been made by Congress under the Freedom of Information Act of 1967 (81 Stat. 54). This Act establishes procedures to expedite the freedom of information by setting up means for any citizen to obtain access to identifiable Federal records (with certain identified exceptions).

Congress has also legislated procedures to expedite the integrity or accuracy of information maintained about individuals. An example here is the right of citizens, under the Fair Credit Reporting Act of 1971 (84 Stat. 1136), to interrogate credit files in order to assess the accuracy of information maintained about them and to demand correction of inaccurate information.

Here, in Information Management then, major current concerns are:

- Feasibility of design of Information Systems that simultaneously meet legislative and judicial requirements for confidentiality of information, freedom of information, and integrity of information.
- Costs to the service industries, government and the public of information systems that satisfactorily meet these three potentially conflicting public demands.

THE LINKAGE BETWEEN PRIVACY, CONFIDENTIALITY AND SECURITY

The linkage between privacy, confidentiality and security rests on the tenets cited earlier, namely:

- *Privacy* is a property of individuals
- *Confidentiality* is a property of data

- *Security* is a property possessed by hardware and software systems and facilities.

Although each of these properties are distinct they are interrelated. Privacy is usually defined in terms of the controls an individual may exercise over the collection and use of information about himself or in absolute terms of forbidden collection and disclosure of information about individuals. One has, for example, the statements that:

- Certain national defense information can only be disclosed to specified individuals.
- A wife may not be forced to testify about her husband.
- In some states a psychiatrist may not be forced to testify about information provided by a patient.
- An individual must be allowed access to his credit record under the Fair Credit Reporting Act.
- An individual may request that his phone number be unlisted.
- A private company (a corporate person) may classify certain information about itself as proprietary and subject to trade secret protection.
- A person may specify that certain information is not accessible until after a certain time, e.g., as in wills.

Privacy of individuals when proscribed as in the above instances immediately translates itself into confidentiality characteristics of data. Confidentiality characteristics of data may be generally defined in terms of:

- The source of the data,
- Allowable recipients of the data,
- Listings of those who have had access to the data, and
- Time periods for which the data is valid.

Compliance with protective rights afforded to privacy of individuals normally then is dependent upon a proper translation of these rights of privacy into confidentiality characteristics of data. Each datum or piece of data will carry along with it a set of tags defining its confidentiality.

Information management must include established procedures for collecting, storing and interpreting for accessibility purposes these confidentiality tags. Compliance with these confidentiality conditions is an important function of information management. It is also costly in terms of obtaining and verifying the confidentiality conditions, of storing them and of

accessing the conditions each time information is requested from the information system.

Once privacy rights have been established by judiciary and legislative processes and once these rights have been translated into confidentiality conditions for the collection and use of information, safeguards and procedures must be established for handling the information in accord with the required conditions of confidentiality. The set of established safeguards and procedures defines the security of the information system and its facilities.

The security of an automated information system or facility, defined in terms of safeguards or procedures, is implemented through:

- Administrative procedures,
- Equipment features and configurations,
- Communications safeguards, and
- Program or software features.

The least expensive and most effective way of providing the necessary security is to know the confidentiality conditions in time to reflect them in the design and development of the system and the facility. This is not, obviously, the typical case today. There are over 110,000 computers being utilized in the United States. The overwhelming majority of these do not possess the security to meet the data confidentiality conditions required by laws recently passed or pending which state the privacy rights which must be afforded to individuals.

Everyone, then whether a private citizen, a government manager, a supplier of information services, or a supplier of computer equipment and software is faced with the problem of retrofitting automated information systems to meet the new conditions of data confidentiality and the protection accorded to individual privacy rights.

THE COSTS OF PRIVACY AND SECURITY

Paying for privacy and security is not new to the American public. Some 15 percent of the 100 million telephones in the United States have unlisted phone numbers. To obtain this privacy, customers must apply to their telephone company and make a one-time payment of $9.00. The American public is currently paying $135,000,000 for this right of privacy.

Airlines now publicly advertise their passenger rates by stating the fare "plus a nominal security charge". The United States has more

private "back-yard" swimming pools than any other country. We are paying for this recreational privacy far more than any other society. The overwhelming majority of working Americans commute in private automobiles rather than use public transportation. There is a nationwide willingness to pay for privacy in transportation.

Apartment buildings find it a valuable asset in gaining tenants to have security guards, TV monitors in halls and garages, and building doors able to be opened only when triggered by an occupant. These security and privacy costs are openly reflected in rental costs. Banks, stores and offices are increasingly making use of TV monitors both for security and to prevent invasion of privacy.

Individuals who select the services of a private physician as opposed to a clinic or other publicly available medical services pay a known price for "private" attention and care. Private education facilities have always been an accepted symbol of individually financed privacy in education.

Executive placement services provide for the prevention of disclosure that an individual is seeking a change in employment. Individuals who have filed their credentials with such a service are compared with the needs of hiring firms. When a match occurs, the individual is notified and requested whether or not he wishes his name forwarded to the hiring firm. The individual is given control over the release of the information that he is seeking employment.

Advertisements for real estate place great emphasis on the privacy afforded in the properties offered for sale. There is a measurable and direct correlation between price and the degree of privacy.

Already and knowingly then the American public is voluntarily paying for many types of privacy and security, representative of which are phone listings, airline travel, recreation, housing, commuting travel, health, and education.

The economics of information management and hence the costs of confidentiality and security of information in automated information systems, unfortunately, are neither well-understood, well-documented nor well-quantified.

Some of the costs of system and facility security are fairly easy to derive. These include, as discussed earlier, the costs of 1) administrative security procedures, 2) equipment security features and 3) communications safeguards.

Costs of program or software security safeguards still need to be derived on a case-by-case basis as do certain of the costs of changes to computer system architecture required by security safeguards.

The costs of injecting data confidentiality tags into an information system and storing and retrieving the information so that is meets the safeguards imposed on these data confidentiality tags have to be determined on a case-by-case, system-by-system basis. An example may help to illustrate the factors involved.

AN EXAMPLE OF COSTS OF DATA CONFIDENTIALITY

In order to respond to the privacy concerns which are embodied in part in the current proposed legislation before Congress, significant changes will have to be made in the way current personal data systems are designed and operated. File sizes will grow and processing and security capabilities of existing computer systems will have to be augmented. Organizations will incur additional administrative costs such as those of corresponding with the individuals about whom they maintain information as well as costs of educating their staff concerning security procedures and its responsibility for individual privacy.

As a concrete example, one might consider the impact of responding to these concerns in a hypothetical credit reporting agency's system. Such an operation may have a file of one million records, each of which typically contains 220 characters of truncated data. These same records contain an average of 330 additional characters representing the six most current transactions on postings to the record. Turning to the specific impact which privacy safeguards would impose, we must first consider that the 220 characters of truncated data are not sufficient to privide for unambiguous identification of an individual. This size will have to be significantly increased, say to about 440 characters since personal identification numbers are not presently used. Likewise, one must provide additional information in each record such as a complete history of all accesses to the record, any access limitation which may be imposed on data within that record, and tags to indicate the age of the information, when it may or must be deleted and

when it may be given out in answer to an inquiry.

In this hypothetical model such changes would result in an average file growth of 10 percent per year, i.e., 33 million additional characters would be added each year so that in seven years the size of the file would double. This growth is due totally to requirements for data confidentiality and does not reflect any file growth due to increase in substantive material. Such growth will clearly affect the operations of the data system. As file size increases and as additional checking procedures are implemented in the software, a price will have to be paid in increased processing time for each query. Larger files will also mean additional hardware. One can thus envision a significant cost for safeguarding data confidentiality.

ALLOCATION OF PRIVACY AND SECURITY COSTS

The question of allocation of these costs between the supplier industries, the service industries, the consumer public and the government has rarely been directly addressed. In the examples cited earlier of privacy and security already accepted or desired, the cost allocation schema vary widely.

The Federal government, for example, shares with the consumer the costs of privacy in education, health and travel. The consumer generally bears the entire costs of privacy and security in recreation, housing and phone listings.

The allocation of costs to guarantee individual privacy in information systems maintained by the credit and banking industry should presumably be handled differently than the costs of ensuring privacy through security and confidentiality safeguards imposed on government information systems.

Under any circumstances, an important action that needs strong support now is the determination, service-by-service, of the costs of individual privacy and decisions on how to allocate these costs.

INFORMATION SYSTEMS, SECURITY INCIDENTS, AND EXISTING THREATS

In resolving the problems of confidentiality and security, any approach taken is dictated by the

facts that: large numbers of information systems already exist in which the necessary safeguards are not present, the technologies on which rest the resolution of the many components of the problems are in widely varying states of readiness, and the threats to information systems differ markedly in their popularity of use.

Existing files maintained by public and private organizations include:

AGENCY	SIZE of FILE
Navy personnel management	1,400,000
Civil disturbance file	13,000
Organized crime	200,000
FBI's National Crime Information Center	5,014,385
National Driver Registration Service	2,600,000
Bank of America individual accounts	14,000,000
TRW Credit Data	30,000,000
R. L. Polk & Company mailing list	200,000,000

The following table of numbers and types of security incidents involving automated information systems during the period 1964-1972 was compiled by Stanford Research Institute.

CATEGORY of INCIDENT	NUMBER of INCIDENTS
National risks	—
Sabotage	15
Theft	23
Copying (data)	8
Tampering[1]	23
Masquerading	2
Browsing/snooping	—
Fraudulent activities[2]	5
Total	76

1 Example: an individual replaces a bank's regular deposit slips with slips that have been "doctored" to show the individual's own account number: walk-in depositors using the "doctored" slips are actually depositing money in the interloper's account.

2 Example: A "computer dating firm" that has no computer. A "computer training school" that has no computer.

Threats to information systems range over a broad spectrum including events such as: natural catastrophe, sabotage, theft, bugging, accidental disclosure and physical assault. The countermeasure spectrum is just as extensive, for example: physical barriers and guards, passwords and identification badges, data encryption, audit trails, personnel practices, backup copies of data, and access control software. Not all threats will exist for each system, and not all countermeasures are appropriate to counter each threat. Each information system must be analyzed to design an adequate security environment.

It is only when armed with these types of data and knowledge that an appropriate approach to the problems of data confidentiality and security can be formulated.

AN APPROACH TO THE PROBLEMS OF CONFIDENTIALITY AND SECURITY

Any realistic approach taken to meet the problems of data confidentiality and computer system security will be multipronged in nature. Minimally, it will be comprised of parallel efforts to:

- Introduce uniform operating practices and procedures where the supporting technology is adequate.
- Conduct coordinated research and development efforts where the necessary science and technology does not exist so that nationwide benefits will result from non-duplicative and widely needed R&D efforts, and
- Apply available technology in systems and procedures in innovative ways which will result in widespread use of these new applications.

The establishment within government as well as in the private sector of uniform administrative and physical security procedures is an example of the first type of effort listed. Here, for instance, the National Bureau of Standards intends to provide by the first quarter of Fiscal Year 1975 a set of guidelines for achieving physical security within Federal automated information systems. An initial survey of feasible physical security procedures and guidelines to be used as a basis for these Federal-wide guidelines has been completed and will be published this year.

A number of very obviously needed safeguards for data confidentiality and system security

cannot be presently implemented because the supporting science and technology is not adequately developed. These problems must be handled as coordinated R&D programs as cited in the second type effort above. One example is that of operating system software which can effectively control access to the information resident in automated information files and the equipment units making up an automated information system.

Another example is that of combating with technology the greatest threat to computer systems — human ingenuity. One way of reducing this threat is through the development of means of uniquely identifying individuals accessing an automated information system in ways that still meet all the judicial and legislative actions prescribed for protection of individual rights. Technology has yet to produce such acceptable identification procedures.

Examples of means for unique identification which generally appear to rely on identification through personal characteristics include: memory passwords, fingerprints, finger lengths, voiceprints, facial appearance, eye iris, picture badges, magnetic stripe cards, and optical ID cards.

An instance of the innovative applications of existing technology which illustrates the third type effort listed earlier in any realistic approach to the confidentiality problem is that of combating the most dangerous external threat to a computer system. This is the remote terminal operated by a clever, computer-knowledgeable individual. Outside the computer's physical barrier and without fear of surveillance, this individual can plan and execute sophisticated probes of the system to discover and later retrieve or modify information in the system. In a computer network, one computer can be used to subvert another. The possibilities are endless, and, to some, intellectually challenging.

DATA ENCRYPTION AS A SAFEGUARD FOR CONFIDENTIALITY AND SECURITY

The application of encryption techniques is an instance of innovative application of technology in civilian information systems. Data encryption will protect data during transmission between a computer and its terminals or other computers. Passwords can be encrypted: so also can data in storage, although the

economics of this latter procedure are highly questionable.

The introduction of encryption will necessitate modifications to terminals, to software, to communications procedures and to system equipment itself. It presently appears, nevertheless, to be the best way to achieve certain necessary confidentiality safeguards.

Data encryption, also called enciphering, scrambling and privacy transformation, is achieved through the use of encryption algorithms. A computer data encryption algorithm can be thought of as a function which translates data into a form which has no resemblance to its original form. For most applications, an inverse function must exist to convert this encrypted form back to the original. A perfect algorithm is one which is very simple, can be known by everyone, is its own inverse, is based on a simple key known to its authorized users, and requires an infinate amount of work to read the scrambled form without the key. No such perfect algorithm exists. Some examples will bear this out.

An algorithm with perfect security is one in which a purely random key is "added" to the message producing a purely random cipher. The receiver "subtracts" the purely random key in order to obtain the original message. The problem is that such a key must be as long as the sum of all the messages transmitted. This becomes an impossible key distribution problem.

A simple computer algorithm which may be used is a pseudo-random number generator based on multiplying a fixed initial number (the "seed") by the key and taking the result modulo some number 2^N. If $N = 72$, for example, a brute force attack on this algorithm making one test per microsecond on one million of the fastest CDC 7600's available would require 150 years to "break" the key and subvert the system. However, simple analysis of this kind of algorithm by noting the statistical patterns of the results can produce the seed of the generator and hence the key in a much shorter time.

Some commercially available crypto generators are said to use a random code generator of more complexity than the previous example: one such device is said to allow generation of pseudo-random streams in excess of 66 billion bits before repeating. These streams are based on 25 billion different possible key combinations. A brute force attack by an individual to obtain a single key of this machine using the

same CDC 7600 at one test per microsecond would take a full shift of computer time given that the necessary input and output existed and the algorithm were known. Not having all the necessary materials changes the task from very difficult to impossible.

Thus, simple algorithms and equipment can be developed to provide protection against intentional subversion of computer systems. NBS is in the process of making such algorithms generally available in order to achieve required protection and a balance between simplicity, economy, and security. NBS is working with and will need the assistance of both industry and government to achieve this goal.

SUMMARY: PROBLEMS, RESPONSIBILITIES and APPROACHES

Experience seems to indicate that the many problems of individual privacy, data confidentiality and computer security can, in most instances, be tackled simultaneously and resolved in a reasonably scheduled manner.

The problems of settling the problems of *individual privacy,* are the responsibility of courts, Congress and state legislatures. So also is the associated problem of stating penalties for non-conformance. National coherence in legislation and court decisions should be achieved as soon as possible.

Translation of the privacy rights of individuals into conditions of *data confidentiality* is a joint responsibility of each special interest service community, and computer and information technologists. Even without passage of privacy legislation or additional court decisions, useful anticipatory translation is eminently practical.

The confidentiality tags which must be associated with information, such as: data source, allowable recipients of the data, listings of those who have had access to the data, and date of validity of the data, will be differently interpreted by the medical community than by the law enforcement community or the credit service industry.

These different interpretations will result in different file structures, file sizes and access procedures which must be delineated and costed by technologists.

Technological alternatives for retrofitting existing systems and specifying new systems must be

reviewed and mutually agreed upon as acceptable by involved information service suppliers, the legal community and technologists.

Innovative applications of data encryption techniques with governmental sponsorship and support and within as many information service areas as possible can begin during the next year.

Widespread agreement among large groupings of information service suppliers and by managers of large record-keeping segments will ease the adoption of administrative and *physical security* procedures. Adoption of such security procedures and subsequent compliance with them will be a tremendous aid since these are documented now and since there has been considerable experience with their use in specific communities.

Government agencies and private sector groups such as the American Banking Association, the American Hospital Association, and the American National Standards Institute can adopt such procedures as guidelines or standards.

RESEARCH and DEVELOPMENT

A general consensus can be reached by government agencies and by private sector service groups on their most important needs which existing science and technology cannot fulfill. This will allow for separate but coordinated R&D efforts with nationwide benefits.

Examples presently seem to include means of unique identification of individuals, redesign of operating system software and computer network protocol development.

Federal, state and local governments have much to gain by coordinating R&D efforts: so also do private sector groups. This is especially true since some of the research, such as that for unique individual identification, will be long term, expensive and not profitable enough for any single company to warrant total industry funding.

ECONOMIC and COST PROBLEMS

There is presently no reliable estimate of what "the traffic will bear" in paying for the costs of individual privacy or information system security.

Costs, as well as legitimate and acceptable ways of allocating these costs among consumers, government and industry, need to be deter-

mined by task forces of economists, technologists and management.

Cost determination is an essential and early ingredient of any plan for achieving individual privacy and its attendant confidentiality conditions and security safeguards.

CONCLUDING COMMENTS

The privacy problem has already introduced serious stresses between society and technology. The best that can be striven for now is to allay present tensions and reduce the follow-on problems of the future. The visible assumption of relevant responsibilities by government and service industries and correlative progress in protection of individual privacy by the courts, Congress and legislative bodies in the country is perhaps the only first step that will permit subsequent resolution of the privacy problem.

That first step is what we are all striving for today.

REFERENCES

(1) Bell, Daniel, "The Management of Information and Knowledge" *The Management of Information and Knowledge*, Committee on Science and Astronautics, U.S. House of Representatives, 1970, pg. 13-15.

APPENDIX 5

Taken From Fips Pub 31—Guidelines for Automatic Data Processing Physical Security and Risk Management in Publication by NBS—Action Summary

The essential recommendations from this publication are summarized here to show the scope of these guidelines and to provide a quick overview of action items in establishing, implementing and maintaining a physical security program in an ADP facility.

I. Organize the ADP Physical Security Program

Assign responsibility for ADP Physical Security and establish a task force to prepare a plan for the ADP security program.

Perform a preliminary risk analysis to identify major problem areas and select interim security measures as needed to correct major problem areas.

II. Conduct A Risk Analysis

Estimate potential losses to the ADP facility and its users from (1) physical destruction or theft of physical assets; (2) loss or destruction of data and program files; (3) theft of information; (4) theft of indirect assets; and (5) delay or prevention of computer processing.

Estimate the probability of occurrence for potential threats and their effect on the ADP facility in terms of the five classes of loss potential.

Combine the estimates of loss potential and threat probability to develop an annual loss expectancy.

Select the array of remedial measures which effects the greatest reduction in the annual loss expectancy at the least total cost. Remedial measures will include: (1) changes in the environment to reduce exposure; (2) measures to reduce the effect of a threat; (3) improved control procedures; (4) early detection; and (5) contingency plans.

III. Determine Local Natural Disaster Probabilities

Evaluate the fire safety of the ADP facility (building location, construction, occupancy and housekeeping) and provide required fire detection and extinguishment, and possibly a trained fire fighting brigade.

Evaluate the exposure to flooding from internal and external sources. Where needed, provide flood protection for the building, relocate ADP hardware, reroute plumbing lines and provide water damage/flood-control equipment (pumps, tarpaulins, etc.)

Evaluate resistance of the building to wind and water damage if exposed to hurricanes, tornadoes or other high winds.

IV. Initiate A Security Program

Prepare a plan and a schedule for implementing selected remedial measures.

Prepare and maintain a policy and plans handbook to include: (1) an ADP physical security policy statement; (2) mandatory security procedures; (3) security guidelines for system design, programming, testing, and maintenance; (4) contingency plans; (5) security indoctrination materials; and (6) a security audit program.

V. Protect Supporting Utilities

Estimate the number and duration of electric power transients, undervoltage conditions and power interruptions and their annual loss expectancy. Install appropriate protective equipment such as: voltage regulating transformers, dual power feeders, uninterruptible power supplies, on-site power generators and ADP power isolation circuits.

Estimate annual loss expectancy from air conditioning failures considering required operation schedules, annual profiles of local temperature and humidity, and an estimated number and duration of air conditioning failures. Where necessary, increase reliability with redundant equipment, provide for emergency use of outside air and augment maintenance capability to decrease mean time to repair.

Estimate the annual loss expectancy from teleprocessing circuit failures. Where cost is justified, increase reliability with redundant communications cir-

cuits and augment repair facilities to decrease the duration of interruptions. Software should be designed to minimize the impact of errors caused by communications failures.

Determine if ADP operations could be interrupted by the failure of other supporting utilities such as water, natural gas, steam, elevators or mail conveyors. If necessary, take steps to increase reliability and decrease the mean time to repair.

VI. Optimize Computer Reliability

Perform a failure analysis to estimate the number and duration of significant hardware failures and their impact on ADP operations. Estimate the annual loss expectancy from delays in performing urgent ADP tasks. Where cost is justified, increase system reliability by adding peripherals, multiple configurations, etc. Review maintenance facilities. Record and analyze all hardware failures in order to identify failure trends promptly and optimize preventive maintenance.

VII. Provide Physical Protection

Identify critical ADP areas including the computer room, data control and conversion area, data file storage area, programmer's area, forms storage area, maintenance area, and mechanical equipment room, and then provide adequate physical protection and access control.

Protect against theft, vandalism, sabotage, espionage, civil disorder and other forced intrusions with improved lighting and intrusion detection systems, with physical barriers at doors, windows, and other openings, and with guards as required.

Control access to critical areas and ADP facilities with conventional or electronic door locks; supervision by guards or receptionists over movement of people and materials; administrative procedures (sign-in logs, identification cards or badges, property passes and shipping/receiving forms); and other regulations.

VIII. Add Internal Procedural Security

Determine potential targets for fraud, theft or misuse of resources by analyzing the work flow and the nature of ADP tasks performed. Incorporate procedures which will minimize exposure to loss. Such procedures may include (1) requiring cooperation between two individuals to perform critical tasks; (2) performing additional checks and bounds comparisons; (3) formalizing standards for high risk operations; and (4) independent quality control checks.

Designate critical positions in ADP management, system programming, program library control, input/output control, exception processing, applications programming, data base management, quality control, internal audit and hardware maintenance and require appropriate pre-employment screening.

Train and supervise all ADP personnel to assure understanding of, and compliance with, internal controls.

Implement control and record keeping procedures for job initiation, scheduling and distribution of output to prevent unauthorized processing.

Control access to physical data files to assure that data integrity is maintained, storage media are protected, custody of data files is traceable and their unauthorized use is prevented. Manual and automatic audit trails should be utilized.

Establish policy and procedures for program and data file retention to satisfy requirements for (1) backup operation; (2) compliance with applicable statutes and regulation; (3) audit and management review of operation; (4) statistical analysis of operations; and (5) resolution of data integrity problems.

Implement programming, testing and documentation standards which satisfy requirements for (1) audit capability; (2) automated acceptance testing; (3) control of program maintenance; (4) quality controls on input data; and (5) non-dependence on an individual's knowledge of systems and programs.

IX. Plan for Contingencies

Compile a set of back-up plans which accommodate the expected range of emergency events requiring back-up operation. The objective of such contingency plans is to protect users of the ADP facility against unacceptable loss. Document performance specifications, operation instructions and technical requirements (system hardware and software, program and data files, and preprinted forms) for each emergency operation.

Select and periodically use an emergency backup off-site ADP facility. Participate in establishing their security program.

Provide protection for the source documents, input and output data and programs while using the off-site facility and in transit.

Establish procedures to assure that (1) current copies of needed back-up materials are retained at a secure off-site location; (2) adequate time is available from compatible off-site ADP facilities; and (3) back-up personnel will be available if needed.

Plan for reconstruction of the ADP facility following destruction including specifications of (1) floor space (quantity, live load rating, location, etc. by functional use); (2) partitions, electric power service, air conditioning, communications, security, fire safety, etc.; and (3) ADP hardware, office equipment and supplies.

Coordinate ADP emergency plans for fire, flood, civil disorders, etc. with the facility self-protection plan to ensure life safety, limit damage, minimize disruption to ADP operations, and expedite repair.

X. Develop Security Awareness

Determine the security training requirements for the ADP staff, senior management, building staff, etc.

Select and implement appropriate security awareness techniques such as (1) training lectures and seminars; (2) posters; (3) orientation booklets; (4) amendments to job descriptions making employees responsible for security; (5) publicity for local security incidents, as well as others occurring at similar installations; and (6) rewards for employees who prevent breaches in security.

Establish and publicize punitive measures.

XI. Audit Physical Security

Establish an internal audit team with representatives from the agency's audit, building safety and security, ADP, and users' organizations.

Develop an audit plan and schedule which systematically validates all critical security and emergency measures.

State in the audit report which measures require improvement or replacement. Use a check sheet (problem description, responsibility for action, action required and follow-up) for each major deficiency to assure prompt resolution.

37-583 O - 74 - pt. 2 - 49



NBS TECHNICAL NOTE 809

Government Looks at

PRIVACY and SECURITY in COMPUTER SYSTEMS

U.S.
DEPARTMENT
OF
COMMERCE
National
Bureau
of
Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards [1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of a Center for Radiation Research, an Office of Measurement Services and the following divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Nuclear Sciences [2] — Applied Radiation [2] — Quantum Electronics [3] — Electromagnetics [3] — Time and Frequency [3] — Laboratory Astrophysics [3] — Cryogenics [3].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of a Center for Building Technology and the following divisions and offices:

Engineering and Product Standards — Weights and Measures — Invention and Innovation — Product Evaluation Technology — Electronic Technology — Technical Analysis — Measurement Engineering — Structures, Materials, and Life Safety [4] — Building Environment [4] — Technical Evaluation and Application [4] — Fire Technology.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.
[2] Part of the Center for Radiation Research.
[3] Located at Boulder, Colorado 80302.
[4] Part of the Center for Building Technology.

Government Looks at
PRIVACY and SECURITY in COMPUTER SYSTEMS

A Summary of a Conference
Held at the National Bureau of Standards,
Gaithersburg, Maryland, November 19-20, 1973

Clark R. Renninger

and

Dennis K. Branstad, Editors

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234



U.S. DEPARTMENT OF COMMERCE, Frederick B. Dent, *Secretary*
NATIONAL BUREAU OF STANDARDS, Richard W. Roberts, *Director*

Issued February 1974

National Bureau of Standards Technical Note 809

Nat. Bur. Stand. (U.S.), Tech. Note 809, 47 pages (Feb. 1974)

CODEN: NBTNAE

FOREWORD

Any potential confrontation between society and technology over problems of individual privacy and data confidentiality can be defused by understanding and action. The Conference on Privacy and Computer Security has contributed to both by providing an initial statement of governmental needs and problems and suggesting a broad range of activities for satisfying them. We hope this Conference report will serve as the foundation for a continuing dialogue among the government, automation industries, service industries, and the consumer which will lead to a refinement of this statement and the assumption of relevant responsibilities for achieving effective solutions.

Ruth M. Davis

Ruth M. Davis, Ph.D.
Director, Institute for
Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce

EXECUTIVE SUMMARY

A two-day conference on Privacy and Security in Computer Systems was sponsored by and held at the National Bureau of Standards on November 19-20, 1973. Five hundred and ten people from government, the computer industry, and various public interest groups met to hear presentations of the needs and problems that confront governmental agencies in safeguarding individual privacy and protecting confidential data from loss or misuse.

Lawmakers at Federal, State and local levels of government are increasingly aware of the public's concern over computer-based recordkeeping and its implications for personal privacy. This concern has arisen partly out of fear of the impersonal super-efficient image that computers present and partly out of a reasoned concern over the expansion of governmental recordkeeping activities which computers make possible. Lawmakers are responding to this concern by proposing and enacting laws that are intended to specifically safeguard the rights and interests of individuals by prescribing the circumstances and the manner in which personal data can be collected, used and disseminated.

These legislative actions, if taken unilaterally, present the prospect of potentially conflicting requirements being imposed upon those charged with their implementation. Further, the technological capability needed to assure compliance with these requirements is not generally available. Compounding these problems are increased public pressures to operate governments economically. These pressures foreclose the simplistic solution of using dedicated computers to process confidential data, yet the computer systems presently available for resource sharing provide few techniques for controlling access to confidential data. These interrelated considerations strongly suggest that all of the legislative, technological and managerial solutions that can be brought to bear upon the problems of privacy and security must be effectively integrated so that a proper balance of needs and values in relation to costs can be achieved.

The assignment and acceptance of responsibilities for accomplishing this objective requires a recognition of the separable but interrelated components of the privacy and computer security problems. These may be identified as:

- Protection of the privacy of the individual: a responsibility of the legislative and judiciary branches of government.
- Providing guidelines to assure information management is in compliance with legislative and judicial requirements for privacy: a responsibility of government, management, and industry.
- Development and application of the needed automation and information management technologies and products: a responsibility of industry and the government.

° Assessment and assignment of the costs of Security in Automation: a responsibility of the government, industry and the public.

° Management of information in automated record-keeping systems: a responsibility of management and information management technologists.

While the solutions for safeguarding privacy are to be found in legislative or regulatory sources, solutions for protecting confidential data are found in physical security measures and in the technological safeguards and procedures which permit controlled accessibility to the systems and data.

The broad scope of controlled accessibility precludes simple solutions. It embraces the use of specialized hardware and software with built-in protective features, mechanisms for authorizing access to systems and data, techniques for uniquely identifying individuals who are authorized to gain access, cryptographic devices and encryption algorithms to protect data during transmission among systems, and auditing or monitoring techniques for measuring system events of security interest.

While various techniques for access control exist, there are few guidelines for the application of these techniques. Lacking such guidelines, system users apply protection controls that are either inadequate or excessively costly for the degree of protection they require. The importance of considering the cost of applying security measures cannot be over-emphasized, since security is always a cost vs. effectiveness trade-off. A highly important extension of this managerial concern is the question of how much the public will be willing to pay for the protection of individual privacy and how the incremental cost for security is to be allocated among government, industry and the public.

Major needs for alleviating the problems of privacy, data confidentiality and computer security were identified on an initial basis. A realistic approach for addressing these needs could consist of parallel and coordinated efforts directed toward:

° Achieving a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.

° Establishing uniform management and technical procedures for effectively applying security measures. Important needs are techniques for assessing risks, determining threats and threat sources, evaluating alternative security measures, auditing the effectiveness of existing measures and physical security.

° Innovative applications of existing technology to enhance security effectiveness. Specific needs which are susceptible to solution in this way include the retrofitting of existing systems to satisfy new security requirements and the use of

encryption techniques in civilian applications for protecting data during transmission.

- Research and development of new mechanisms and techniques where significant needs cannot be met satisfactorily by existing technology. Among the needs requiring this type of effort are self-protected computer systems which have the internal ability to enforce the access controls necessary for the prescribed level of security. Other needs include techniques for positively and uniquely identifying individuals who have authorization for access to the system and data and the development of secure network models for evaluating alternative network designs.

- A study of the costs of data confidentiiality and security to build an understanding useful in making public choices about degrees of privacy desired by individuals and for allocating costs among the public, industry and government.

It is hoped that the Conference will stimulate the computer industry and other interested parties to propose specific approaches and solutions to the needs and problems outlined and will promote new initiatives for protecting data confidentiality in computer-based records systems.

A second Conference is planned for March 4-5, 1974, which will provide an opportunity for the presentation of proposed technological and regulatory solutions to the computer security needs and problems identified in this Conference.

TABLE OF CONTENTS

SECTION	TITLE	PAGE
	Foreword	iii
	Executive Summary	iv
	Abstract of Report	1
I.	Introduction	1
II.	Where the Problem Arises	2
III.	The Operating Environment	10
IV.	What's Needed	15
V.	Costs	24
VI.	Action Plans	28
	Appendix A - Conference Program	33
	Appendix B - Publications/References	36
	Appendix C - Preview--March 4-5, 1974, Conference	37

Government Looks At Privacy and Security in Computer Systems

Summary of a Conference held at the National Bureau of Standards, Gaithersburg, Maryland

November 19-20, 1973

Clark R. Renninger and Dennis K. Branstad, Editors

This publication summarizes the proceedings of a conference held for the purpose of highlighting the needs and problems of Federal, State, and local governments in safeguarding individual privacy and protecting confidential data contained in computer systems from loss or misuse. The Conference was held at the National Bureau of Standards on November 19-20, 1973.

The origin of governmental problems is discussed in the context of the public's concern for privacy arising out of computer-based recordkeeping, the diverse legislative actions now being taken to safeguard privacy, the threats to the security of computer-based information systems and the technological problems associated with protecting against such threats. Useful distinctions are drawn between privacy, confidentiality and security to clarify the issues and allocate responsiblities for solving the problem among lawmakers, technologists and management.

Major needs are described. These include the need for cohesive Federal, State and local legislation; technological guidelines and standards for assuring uniform compliance with legislative requirements; management guidelines for identifying and evaluating threats to security; and improved technological mechanisms for controlling access to computer systems and networks. Cost implications of providing security measures are discussed.

Key words: Computer systems, privacy and security; confidentiality; privacy; security.

I. Introduction

1.1. Purpose of the Conference

This paper is a summary of a two-day Conference on Privacy and Security in Computer Systems, held on November 19-20, 1973, and sponsored by the Institute for Computer Sciences and Technology of the National Bureau of Standards.

In his introductory remarks, Dr. Richard W. Roberts, Director, NBS, indicated that the Conference was attended by 510 people: 375 of them from Federal, State and local governments, and 135 from the private sector. These attendees represented 7 Congressional offices, 46 Federal agencies, 30 States, 7 local governments, 34 computer companies and 41 professional associations, universities and public interest groups.

The stated purpose of the conference was to:

531-845 O - 74 - 2

"Identify initial requirements and issues that confront governmental organizations in safeguarding individual privacy, data confidentiality and computer security.

"Communicate this information to groups in the public and private sector in order to mobilize and orient efforts that can respond to recognized needs.

"Establish a foundation for a second conference to be held on March 4-5, 1974, which will provide the opportunity for the presentation of proposed technological or regulatory solutions to the computer security needs and problems identified in this Conference."

1.2. Organization of the Summary

This summary identifies the principal themes of the various presentations and organizes them to:

A. Identify the origins of the problems encountered by Federal, State and local governmental bodies in attempting to meet their responsibilities in safeguarding information needed to perform governmental functions.

B. Describe the milieu in which they operate.

C. Describe the problems as seen by Federal, State and local governments.

D. Discuss the issues of costs.

E. Present suggestions for action.

The summary is an integration of the papers and presentations of the Conference. In all cases, it is believed that the intent of the speakers has been preserved.

1.3. Appendices

A. The Conference Program

B. References to source materials cited at the Conference

C. A preview of the March 4-5, 1974, conference

II. Where the Problem Arises

2.1. Public Interest

In the keynote address, John K. Tabor, Under Secretary of Commerce, noted a number of factors that are creating pressure for solutions to the problems of providing protection to confidential or valuable data against misuse or loss. He cited the general expansion of government and private information gathering and recordkeeping to support the needs of

society as a phenomenon of recent American life. The capability to manage large recordkeeping activities and derive useful data is made possible and even accelerated through use of computers. He noted that linking computers through telecommunications multiplies the capability to exchange and share the results of information-collecting activities while at the same time compounding the protection problem. Under Secretary Tabor called for soundly designed safeguards to protect the confidentiality of data collected in support of expanded services and programs at all levels of government.

Congressman Jack Brooks, Chairman of the Government Activities Subcommittee of the House Committee on Government Operations, noted that control over dissemination of such information involves two concepts: privacy, or who should have access to what information for what purposes; and data security, which prevents unauthorized access to the data and also protects its integrity.

In discussing the large number of data banks involving personal data that already exist, Congressman Brooks indicated that 7500 data banks were counted in the Federal Government alone; he further indicated that he believed the count was "low." The number of non-Federal data banks involving personal information is unknown although it was indicated that the State of California has between 8,000 - 10,000 data bases of which approximately 45% (3,600 - 4,500) involve personal data. While these figures represent only two very isolated data points, it is evident that the number of Federal, State and local government data files containing personal data is very large indeed. Coupled with the large or even larger number of files containing personal data to be found in the private sector (e.g., insurance companies, credit card plans, mailing lists, school records, etc.), this represents a very large pool of information that is being actively collected and maintained.

Along with the intensified recordkeeping activities of governmental units has come an increased awareness of the part of the public that such activities are going on, and with this awareness there is an increased sensitivity about individuality and personal rights. It would be stretching facts to suggest that the rise of awareness and feeling of potential threat to one's individuality comes from abuses in the collection and use of data by governmental units. Rather, it would seem that such awareness comes about from a variety of factors present in an increasingly complex society. Regardless, the public's desire for privacy is quite real and has created a conflict between the interests and rights of an individual and the interests and rights of government (and private) institutions. As David B. H. Martin, Special Assistant to the Secretary, HEW, pointed out, this conflict of interests raises the public policy questions that require legislative and regulatory solutions.

Congressman Brooks pointed out that no legislative action can be effective without the corresponding technological advances to support legislative efforts. He said, "The directives of Congress and State legislatures as to constitutional and social restrictions to protect the

rights of individuals will be of little consequence if the data itself is readily available to ill-willed persons using surreptitious or unlawful means."

It is clear that legislators are concerned about the question of rights of individual privacy. They are willing to support legislation that defines these rights and attempts to strike a harmonious balance between the rights of individuals and the rights of society as a whole acting through various institutions and agencies of government.

Dr. Alan Westin, Professor of Public Law and Government, Columbia University, in an interesting review of the international aspects of the privacy question, identified three phases of awareness and action:

a) Early Warning Phase - the crying of public alarm and rising public awareness of the conflict between organizational efficiency and privacy.

b) Study Phase - commissioning of studies to identify the problem.

c) Regulatory Phase - the development of administrative, legal and regulatory safeguards for privacy.

He indicated that most of the Western industrialized nations have passed beyond the initial phase and have moved into the Study and Regulatory Phases, while at the same time the issue is just being recognized in nations with different cultural backgrounds, such as Japan.

In commenting on some 7 - 10 studies performed in a variety of countries, he noted their remarkable similarity, taking into account the differences in terms of reference and cultures. The more significant common findings included:

a) Computer technology increases the efficiency of recordkeeping.

b) There is significant fear (of loss of privacy) on the part of the public.

c) None of the studies could document specific episodes where automated record-keeping created new loss of personal liberties. (Any abuses that were uncovered had existed in pre-automation manual record-keeping times.)

d) Use of computers intensifies problems (of policy, etc.) that existed in manual systems.

e) All of the reports recommended protective measures to protect individual rights.

Those countries having advanced to the regulatory phase appear to be evolving three patterns of approach to regulation. These were summarized as administrative self-regulation (the British approach), omnibus licensing and regulation (Swedish-German approach) and area-by-area provision of court enforceable citizen rights (the U.S. approach).

2.2. Separable Issues

There is a tendency to confuse the issues of privacy, confidentiality and security with respect to recordkeeping and computers. Dr. Ruth Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards, outlined the essential differences between these issues and established a framework for unambiguous discussion and solution of these problems.

Privacy is a concept which applies to individuals. In essence, it defines the degree to which an individual wishes to interact with his social environment and manifests itself in the willingness with which an individual will share information about himself with others. This concept conflicts with the trend toward collecting and storing personal information in support of social programs of various importance. The government's role often makes the supplying of this information mandatory--thus, creating a direct and acute compromise of the individual's privacy. Under this circumstance, the burden of protecting personal data is all the more important.

Confidentiality is a concept that applies to data. It describes the status accorded to data and the degree of protection that must be provided for it. It is the protection of data confidentiality that is one of the objects of Security. Data confidentiality applies not only to data about individuals but to any proprietary or sensitive data that must be treated in confidence.

Security is the realization of protection for the data, the mechanisms and resources used in processing data, and the security mechanism(s) themselves. Data Security is the protection of data against accidental or unauthorized destruction, modification or disclosure using both physical security measures and controlled accessibility techniques. Physical Security is the protection of all computer facilities against all physical threats (e.g., damage or loss from accident, theft, malicious action, fire and other environmental hazards). Physical security techniques involve the use of locks, badges (for personnel identification), guards, personnel security clearances and administrative measures to control the ability and means to approach, communicate with, or otherwise make use of, any material or component of a data processing system. Controlled Accessibility is the term applied to the protection provided to data and computational resources by hardware and software mechanisms of the computer itself.

From these definitions, it is possible to see that there is no direct relationship between privacy (a desire by individuals, groups or organizations to control the collection, use or dissemination of information about them) and security (the realization of the protection of resources), although they are interrelated. Several speakers pointed out that a perfectly secure computer could be used in such a way as to violate individual privacy. However, this should not be construed as an excuse for not creating secure computer systems since the thrust of earlier remarks was to the effect that legislatively defined rules for

assuring privacy are now levying a security-oriented environment on government (and possibly private) data systems.

2.3. Social Implications

Dr. James Rule, Professor of Sociology, State University of New York at Stony Brook, presented a sociologist's view of the privacy question. He observed that the issues of privacy are social-political-human rather than technological and that the question of how far to go in computer-based recordkeeping on people is a political/social question in which the rights/needs/interests of the individual must be weighted against the rights/needs/interests of "institutions" (social, political, commercial, etc.). In his view, determining the proper balance between individual privacy and institutional needs and interests will involve even more agonizing choices in the future than it does now. To illustrate his point, he described a hypothetical situation revolving around the use of computerized recordkeeping control of crime. In the hypothetical (but potentially feasible) situation, statistical methods of behavior analysis are used to predict individual criminality before it occurs. Assuming that such a system could be assured of evenhanded administration, would such a system be desirable and would it justify the extensive recordkeeping on all individuals necessary to make it work?

2.4. Legislative Actions

As a result of the early warnings and studies of the privacy issue that have taken place in this country over the past 7 - 8 years, a number of legislative actions have taken place or are contemplated. For example, three Federal Acts have been passed in recent years relating to the issue of privacy. These are the Freedom of Information Act, which provides for making information held by Federal agencies available to the public unless it comes within a category exempted by the Act; the Federal Reports Act, which establishes procedures for the collection of information by Federal agencies and the transfer of confidential information from one agency to another; and the Fair Credit Reporting Act, which requires consumer credit reporting agencies to adopt procedures which are fair and equitable to the consumer with regard to confidentiality, accuracy, relevancy and proper use of such information. The Fair Credit Reporting Act also established the right of the individual to be informed of what information is maintained about him by a credit bureau or investigatory reporting agency.

In addition to these pieces of legislation, numerous bills have been introduced in Congress which propose to strengthen the rights of individuals with respect to confidentiality of data, prevent invasion of privacy, establish standards for the collection, maintenance and use of personal data, or limit the uses to which personal data can be put without written consent of the affected individual. It was also reported at the Conference that the Department of Health, Education and Welfare (DHEW) is implementing (internally) the

recommendations contained in the Report of the Secretary's Advisory Committee on Automated Personal Data Systems. (See Appendix B, Ref. 1)

The 50 State governments have pending numerous bills concerned with protection of individual privacy and data confidentiality. Massachusetts and Iowa have already passed significant legislation in these areas, providing higher standards of personal privacy protection than the Federal Government. Still other States have extensive legislative proposals that would impose extensive regulatory and technological constraints on the operation of personal data systems.

At the local level, a number of municipalities have passed ordinances to provide protection of computerized personal data.

While all of this legislative activity is not completed, it is indicative of the political response to the aforementioned public awareness and concern over individual rights and privacy.

2.5. Threats

Threats to individual privacy and technological threats to computer-based information systems were the two themes repeatedly stressed by the various speakers. While the threat to individual privacy and liberty was predominant and seen to be mostly associated with the unregulated collection and use of personal data, a number of the speakers cited the technological threats as being those most bothersome to the operators of information systems.

Most of the speakers agreed that the threat to privacy was one that required legal and regulatory remedies and was not basically a technological problem. All speakers agreed, however, that technology was required to help enforce the legal and regulatory steps. Furthermore, a number of speakers noted that unless there were sound technological foundations for controlled access to computer systems, the legal and regulatory actions would be largely wasted.

In addition to the basic and somewhat diffused threat to individual privacy posed by the collection and use of personal data, several speakers cited an additional problem of misappropriation and misuse of data by people who are authorized access in connection with their jobs. While the problem of misuse of data would appear to be one solved by legal measures providing stiff penalties for violators, several speakers indicated that it was in part technological since the contemporary systems have so little in the way of controlled access mechanisms that it is difficult to restrict access within a data base and to account for its access and usage.

The degree of difficulty and the costs associated with providing security and controlled access to computer-based recordkeeping systems is a function of the type of access being

37-583 O - 74 - pt. 2 - 50

permitted, the capabilities of those performing the access, and the type of computer system (whether dedicated, shared, local or remote access, etc.) on which the recordkeeping system is based. In order to put some of the later discussions of approaches to solving the problem into perspective, the classes of individuals who may access a computer system and/or its information products could be categorized as follows:

> Consumers - a term applied to the authorized recipients of information (products) of a computer-based recordkeeping system. In many applications of computers, this group is the supplier of the raw data as well. In organizational terms, consumers would comprise an operating agency or department.
>
> Producers - a term applied to the analysts and applications programmers who design and implement specific recordkeeping systems which produce information products for consumers. Producers may or may not be a part of the consumer's organization. Producers require access to the computer system to develop products; their programs require access to data in the system.
>
> Servicers - a term applied to the computer operations staff; includes operators, systems programmers, data entry services, etc., responsible for availability and maintenance of the computer system resources. The servicers may or may not be a part of the consumer's organization. Servicers require access to the computer system to operate and maintain the resource. Because they have physical access, they have the capability to access any information in or on a system.
>
> Intruders - a term applied to individuals or organizations who have no authorized access to a computer system or its products and have a possible malicious interest in obtaining unauthorized access to data or a system. Intruders are generally thought of as not belonging to any of the categories above. The primary characteristic of an intruder is his lack of authorized access to any part of a computer system or its products. He is an outsider.

The threat to data confidentiality or system security is related to the capabilities of each class of individuals in dealing with a system and the existence of an asset (data or system) that is supposed to be protected from some or all members of one or more classes. As an example, any system and its data should be protected from intruders. Some (shared) systems may contain data that is meant to be protected from different (organizational) groups of consumers, etc. A simplified view of the degree of threat and the problems faced in protecting data confidentiality and information processing resources is shown in the table and the comments following. The sixteen possible entries in the table have been grouped into ten threat classes.

Type of System / Access Capability As:	Local (off-line) Batch		Remote (on-line)	
	Dedicated	Shared	Dedicated	Shared
Intruder	T_1	T_1	T_2	T_2
Consumer	T_3	T_4	T_5	T_6
Producer	T_7	T_8	T_7	T_9
Servicer	T_{10}	T_{10}	T_{10}	T_{10}

T_1	Intruder versus Batch	Threat is a function of physical security measures and their enforcement. High degree of risk of exposure to intruders.
T_2	Intruder versus Remote	Greatly expanded threat of unauthorized access due to potential vulnerability of communications. Low risk of exposure. Potential for masquerading as any of the authorized users quite high.
T_3	Consumer versus Dedicated Batch	Threat to data confidentiality primarily that of misusing data otherwise authorized for access. Access control based on personal identification.
T_4	Consumer versus Shared Batch	Same as T_3 plus risk of misdirecting data; control of access to data (products) generally based on personal identification by operations staff. Procedures to assure proper data handling must be available and strictly enforced.
T_5	Consumer versus Dedicated Remote	Somewhat expanded threat because of substitution of automated methods for personal identification. Also must validate identity of terminals. Requires either physical access controls for terminal area or authenticated identification of user. Increased costs of administration to control physical access to terminals and/or authenticated identification method.
T_6	Consumer versus Shared Remote	Same as T_5 with increased opportunity to masquerade if identifier/authenticator is compromised. Risk of data misroute present.
T_7	Producers versus Dedicated Systems	Producers constitute roughly the same threat as consumers except that they have the technical capability to siphon off data through corrupted programs. Degree of threat is a function of where they reside organizationally. If under same management control as consumers, threat is about the same as the consumer threat.
T_8	Producers versus Shared Batch	An increased threat to data over T_7 but generally dependent on the operating system design. Can frequently spoof the operating system to gain unauthorized access to data.
T_9	Producer versus Shared Remote	Same as T_8 (and T_7) except greatly reduced risk of exposure plus increased opportunity for anonymous bypass of access controls. Some increased risk of masquerading depending on organization and physical set-up of remote sites.

T_{10}	Servicer versus All Systems	Maximum threat. Generally unrestricted access to any program or data on the system. Greater opportunity and technical capability to access data due to direct physical access to the computer system.

III. The Operating Environment

3.1. Introduction

It would be impossible to enumerate all of the data systems involving personal or otherwise valuable data or resources. However, in order to provide an operational framework for discussion of the privacy and security issues, the Conference did provide illustrations of such personal recordkeeping functions in governmental units and the kinds of data confidentiality and computer resource security problems that are faced by Federal, State and local governments. No significance should be attached to the order in which these illustrations appear.

3.2. State of California

Mr. Kent Gould, Chief, EDP Development, Department of Finance, State of California, described the organization of data processing in California. California expects to spend approximately $100 million for data processing activities in 1973, a figure that is growing at the rate of 20% per year. Eighty (80) state departments and agencies use data processing equipment for just about every application conceivable except command and control. The Department of Finance has absolute EDP authority in California, approving individual DP budget requests for equipment and personnel. In this role, the Finance department has the responsibility for enforcing compliance with security and privacy requirements.

California is presently attempting to consolidate data processing activities into five (5) major centers. Gould estimated that between 8000 and 10,000 data bases are processed by the State of California, of which approximately 45% contain personal data. He estimated that it costs between $200,000 and $400,000 per center to provide for security and privacy requirements.

In reviewing the privacy issue as seen in California, Gould indicated that it is the responsibility of the legislature to provide policy direction in this matter and to identify the confidentiality requirements of various data. Where there is no legislative mandate, the Executive branch will take action in its best view of the problem to protect data from unauthorized dissemination and use. It will monitor the data processing practices to insure that confidentiality requirements are met. In connection with the last point, he mentioned that California was developing a master audit package that "correlates to security/privacy requirements" and will be used to measure security/privacy compliance by the operating departments and agencies.

Finally, he noted that the primary security/confidentiality problem in California is how to prevent unauthorized use of data by people having authorized access to it. The essential question is the balance between management responsibility and public responsibility.

3.3. Law Enforcement Assistance Administration

Mr. George Hall, Acting Assistant Administrator, Law Enforcement Assistance Administration, Department of Justice, reviewed the development of LEAA's activities in the development of computerized criminal information files. This activity was conceived as a network of State defined and operated systems dedicated to maintaining criminal activity information. The project grew from a feasibility demonstration project, SEARCH, that had 20 States participating by sharing criminal histories through a central data index. Hall noted that the development posed a number of design and policy questions of serious import to the question of privacy and constitutional rights of individuals. As a result of serious consideration of the problem, it was decided that: (a) the system(s) should be decentralized to eliminate the appearance (and reality) of Big Brother data banks; (b) only "serious" offenders should be included in the files; (c) only criminal and public record information should be kept. He noted that the policy decision to decentralize the system(s) has added to the costs of privacy.

In discussing the problems currently perceived with the system, a number of important problems/questions impinging on the issues of privacy/confidentiality/security were noted. Specifically, he cited the problem of who should be able to access criminal history data as one that needs joint Federal/State legislative action. Currently, most State statutes permit virtually anyone to access the records. Another problem is the integrity and validity of the data itself. Arrest records are maintained, but the disposition of the arrest is often not entered. In order to maintain properly valid and accurate data in such systems, it may be necessary to create <u>new</u> information collection systems (a move that appears to complicate the problem). Still another problem is the right of the individual to access and/or validate his records, along with questions of how long such records should be maintained. Finally, the question of file separation or merging for efficiency reasons looms large as a potential <u>future</u> danger to civil liberties.

(NOTE: The comments and problems noted above are better understood in the perspective of LEAA activity in this area. A review of LEAA's activity and other government activity in developing and maintaining criminal information files can be found in Appendix E of the HEW report.)

Finally, Hall noted a severe need for rational <u>uniform</u> standards regulating the collection and use of information.

3.4. State of Ohio

Mr. Jerry Hammett, Deputy Director, Department of Finance, State of Ohio, gave a brief review of automated recordkeeping activities in Ohio. The Ohio Department of Administrative Services either provides ADP services or authorizes the use of outside suppliers.

In describing data of security concern to Ohio State Government, he cited the following files as typical:

> Personal Income Tax Records; Driver's License Records; Arrest and Conviction Reports; VD Records (Department of Health); Patient Records (Mental Health); Government Planning Records for Highways, Buildings, and Recreation.

Indicating that the concern over the security and confidentiality of data is not exaggerated, he cited the case where a Deputy Sheriff in an Ohio county was conducting an investigation business on the side and used his access to State criminal history records to supply data to his clients. In another case, personnel in the Motor Vehicles Department were found to be expunging data of serious traffic violations from offenders' records. He also posed the hypothetical threat of having individual (and corporate) tax liability modified in an unauthorized way.

Hammett stressed his view that interactive processing threatens system security. In discussing directions for possible solutions, he indicated the need for model (and eventually real) legislation concerning privacy and confidentiality and security standards and for the vendors to provide hardware and software security in their products.

3.5. State of Illinois

In a talk on managing computer operations, Mr. Robert Caravella, Management Information Division, Department of Finance, State of Illinois, presented highlights of some of the results of the joint State of Illinois - IBM study of the applicability of IBM's Resource Security System (RSS). He began by noting (as did other speakers) that the HEW study and Canadian Task Force on Computer Security and Systems marked the beginning of a "new era" in providing safeguards for privacy and data confidentiality.

In discussing the need for confidentiality/security provisions, he cited a number of potential (and real) exposures found in contemporary systems. These include:

1. Erroneous or Misleading Data
2. Accidental Disclosure
3. Intentional Infiltration
4. Loss of Data
5. Absence of Established Standards

He then went on to outline an Information "Privacy" Action Plan. The plan outline consisted of the following steps:

1. Review Information System Requirements to Determine:

   what is collected
   why it is collected
   who needs it
   when it is needed

2. Analyze the Confidentiality and Criticality of Information:

   to operations
   for proprietary or other reasons

3. Assess Vulnerabilities and Risks - Establish Tradeoffs between:

   exposures
   value of information
   cost of safeguards
   effectiveness of safeguards

4. Make Security Decisions

5. Investigate Technical Safeguards including:

   software requirements
   hardware requirements
   physical access control(s)

6. Budget for Information Security

7. Organize for Security

8. Establish Individual Accountability

9. Implement Technological Safeguards

10. Create a Security Conscious Environment

11. Issue Policy Statements

12. Audit

Finally, in discussing the benefits to be expected from the joint Illinois - IBM security study, he noted that the project was "well-balanced" in its approach--that the vital areas of legislation, technology, administration and education were all covered in the study. In the legislative area, model legislation has been produced covering individuals' rights to privacy and regulating the collection and use of information in the State. The technology activity was focusing on the areas of performance measurement and cost analysis of using RSS. In the administrative area, the work is concentrated on monitoring the application of RSS to determine how well it meets the needs of State governments and what additional safeguards may be needed. The educational aspect is being served by the development of 10 video tape training programs aimed at diverse audiences from management to the technical support staff of ADP operations.

3.6. Department of Health, Education and Welfare

Dr. Robert Laur, Acting Director, Office of Policy Development and Planning, HEW, outlined some of the unique privacy/confidentiality problems that arise in connection with the operation of the National Center for Health Statistics (NCHS). As one of the major statistical data banks of the Federal government, the NCHS provides statistical services for HEW.

Because of the sensitivity of medical information, NCHS has adopted the isolation of a dedicated system as their approach to the confidentiality problem. The primary problem is that of data confidentiality and the protection of proprietary interests of the contributors of the data. Since the medical data is identified with a Social Security or other identification number, this number is (cryptographically) transformed to protect the identity of the individual, and the transformation key is "carefully controlled."

In support of research, NCHS provides other workers with standardized data tapes obtained from its data bases. The standardized tapes are constructed to remove personal identification and to suppress statistical entries with a small number of samples (in order to eliminate potential identification through advanced correlation techniques). In the end, Dr. Laur noted, they rely on professional ethics for the major control over how sensitive medical data is used.

He also observed that the present NCHS system security/confidentiality controls work well enough for the kind of (dedicated) systems they are now using but that they will not suffice for time-sharing systems and network connections of the future.

Presently, HEW is proposing legislation to establish a common shared information base that would let NCHS use data located at other (medical) centers (or possibly systems supporting health care delivery). This would avoid redundant collection. As an example, he cited the HEW's Professional Service Review Organization that requires correlating diverse medical, hospital and physicians' records to obtain a review. He noted that a single Federal system design for maintenance of health records raises more control problems than it solves.

3.7. Congressional Research Services

In a paper that demonstrated that requirements for data confidentiality are not unique to the Executive Branch, Mr. Robert Chartrand, Specialist in Information Sciences, Congressional Research Services, Library of Congress, provided a review of Congressional Information Protection needs. These needs are determined by the multiple roles played by a member of Congress, and the historical development of how Congress operates. Among the kinds of information cited as requiring protection were:

a) Casework data relating to individual constituents.

b) Political data--contributors lists, key civic groups, mailing lists, etc.

c) Committee/Subcommittee data--legislative planning data, privileged hearings data, etc.

d) Debate Supporting data--privileged information supporting public debate.

Supporting Congress are three computer facilities, one each for the Senate and House and the Congressional Research Service (CRS) of the Library of Congress. The Senate and House systems perform diverse administrative functions and services for the members, while the CRS system supports a variety of information systems on pending legislation, bibliographic information and an issue briefing system.

Typical of the Congressional security controls are those taken by the Library of Congress. The bulk of these are physical security measures including a visual control on computer room access, use of key-cards for after-hours work, tape vaults, burn-bags and the like. Procedural controls cited included separate handling and decentralized control of committee information, use of passwords to protect access to Congressional files, and low information content (generalized) software descriptions.

The future needs of Congress, seen by Mr. Chartrand, include:

- strengthening security provisions of legislative branch regulations
- establishing standards for need-to-know controls for all Congressional users
- description of available data and restrictions on its use
- creation of a Congressional classification system
- creation of an information service group to mediate users' information requests and enforce need-to-know and security regulations
- prepare the most applicable service and control functions which combine protection with inquiry fulfillment.

IV. What's Needed

4.1. Legislative Policies and Regulations

Legislative activity aimed at protecting individual privacy is increasing rapidly at all levels of government. As noted by Dr. Davis, passage of any significant number of these legislative proposals could easily result in an unacceptable morass of conflicting requirements being imposed on regulatory organizations, service industries and automation technology. Some national coherence in these proposals is clearly required if there is to be any realistic or

practical application of the mechanisms needed to protect against intrusions on individual privacy.

Better communication among lawmakers, government administrators, and technologists is also essential because the effective implementation of privacy legislation depends heavily upon the availability of technological safeguards that can assure compliance with a reasonable degree of certainty and uniformity. As several speakers pointed out, it may not always be possible within the current state-of-the-art to respond to legislative requirements of the type being proposed at an acceptable cost. As Mr. Gould stated, a requirement, for example, to record every access to a file involving personal data, if strictly enforced, could cause the file to double in size rapidly. Such growth clearly affects the operations of the system and inevitably leads to additional hardware and more complex software. Early coordination among lawmakers, administrators and technologists should enable impacts of this type to be taken into account in arriving at effective and reasonable legislative policies and the standards and guidelines required for implementation.

This general theme was supported by spokesmen at State and local levels of government. Mr. Andrews Atkinson, Superintendent, Cincinnati/Hamilton County Regional Computer Center, cited the need for regulations governing information management practices as they apply to data collection, storage, application, accessibility, integrity and accuracy. Mr. Carl Vorlander, Executive Director, National Association for State Information Systems spoke to the need for standards for defining categories of data requiring protection and the degree of protection required by each category.

4.2. Management and Operating Guidelines

4.2.1. Determining Information Content

Underlying the process of information management is the need to determine what information is required to carry out the function being performed and to assure that only information which is relevant and essential to that function is collected and processed. The weeding out of nonessential confidential information through this process obviously contributes directly to easing the problems of privacy and data security and thus represents a management activity that should be pursued vigorously and continuously. The processes of security management, as discussed in the Conference, exclude questions of information content but recognize them as important and interrelated considerations which must be addressed.

4.2.2. Evaluating Risks, Threats and Security Techniques

Assuming that the essentiality of the data to be protected has been determined, management guidelines or operating procedures are needed for the effective employment of proper security measures. Particularly needed at this time are guidelines for determining the level

of confidentiality or criticality of information (i.e., what degree of protection is required for proprietary, personal, high value or sensitivity reasons). Of equal importance, as noted by Dr. Walter E. Simonson, Associate Director of Electronic Data Processing, Bureau of the Census, are guidelines for assessing the risks and threats to security, identifying the assets to be protected and evaluating the relative effectiveness of alternative safeguard measures in providing that protection. Dr. Simonson emphasized that employees constitute a major potential threat and suggested the use of pre-employment screening to minimize this risk.

A variety of management techniques exist for valuing assets; and if that were all of the problem, it would be a straightforward actuarial problem to design the required level of security. However, when data confidentiality is part of the security problem, factors other than simple asset replacement costs have to be considered. Some of the factors involved include the degree of threat posed by different potential accessors of a system, as was discussed in Section 2.5.

The specific techniques to be used obviously depend on the degree of threat (or on the degree of confidentiality or importance of the data being protected). Most systems have only the most rudimentary controlled accessibility features. While it can be argued that the cost of providing protection techniques to a data base should be borne by the application(s) requiring them, the design of contemporary systems too often permits such controls to be bypassed completely by anyone with a programming capability. Where the systems are used with a clear and strict distinction between consumers of information and producers of the applications, various data base protection techniques can protect data from unauthorized access by consumers. In many systems, consumers are often producers as well.

However, there are many questions that must be resolved even where the consumers are distinct from the producers. Whether the computer-based protection techniques should be applied on a per-application basis or whether these techniques should be an integral part of the operating system are questions that management of data centers need trade-off evaluations to answer.

The relatively simple question of how to represent authorization to use a data base becomes quite complex depending on the level of detail to which the authorization must apply--file, record, or field within a record. Methods for representing such authorization must be designed and evaluated in the context of the organization and intended use of data bases. Equally important, the management and administrative procedures to update, review and otherwise control the authorizations need to be developed for the technique(s) chosen.

Currently, most of the effort to provide such controls is carried out by the users of data processing systems. Whether they or the suppliers of data systems should develop such protection mechanisms, the fact remains that data center managers have no guidelines as to which kind of controlled accessibility techniques to use under different circumstances and no

statements of the assumptions underlying assertions of protection provided by any particular technique.

4.2.3. Physical Security

The objective of physical security is to keep intruders away from data processing and information resources, as well as to protect the resources from natural hazards. Mr. Ike Friedlander, Executive Director, Public Building Services, GSA, noted that physical security is the foundation of nearly all other security solutions. If physical security measures are not taken, then external penetration of systems can easily occur, making most other measures of doubtful value. He stated that technological detection systems are being used more frequently because of the increasing costs of using human guards. In new construction, physical security is an important design criterion. In some cases, such as a new government building in Seattle, the security system is controlled by a dedicated computer.

The major emphasis in physical security technology is the development of products designed to reduce the cost of a human guard force by providing means to supplement or extend their capabilities. Thus one finds the increased use of closed circuit TV, ultrasonic and other alarm systems, walkie-talkies, smoke and heat detectors of various kinds and the like.

Interestingly enough, there is little in the way of new technology needed for physical security. Mr. Nicholas A. Chronis, Chief, Data Processing Computer Center, Civil Service Commission, pointed out that "the technology exists if the money is available." The major need he see is for Federal guidance on how to provide day-to-day physical computer security. The National Bureau of Standards is planning to publish such guidance early in 1974.

4.3. Controlled Accessibility

Mr. Walter W. Haase, Deputy Assistant Director, Information Systems, Office of Management and Budget, summed up the focus of controlled accessibility in his introductory remarks at the Panel on Controlling Access to Systems and Data when he said:

> "I believe that proper application of existing computer, communication and information processing technology can reduce the threat of improper disclosure of private and confidential data. I also believe that further development effort is required to close the gap between access control needs and available technological solutions. I am not suggesting that technology can provide a solution to the basic privacy issue but that it could reduce the intensity of the conflict."

As described by Dr. Dennis Branstad, Computer Security Project, National Bureau of Standards, the term "controlled accessibility" embraces the technological measures available to control the access of people to a computer system's data and computational resources. These measures include specialized hardware and software, access procedures, authorization

mechanisms, identification methods, and encryption algorithms. Only computer-based mechanisms can provide the rapid response decisions needed for effective access control.

In discussing what is needed to protect data confidentiality in computer-based record-keeping systems, Mr. Daniel Edwards, Research Engineer, NSA, and Mr. Howard Lewis, Manager, Data Management Programs, AEC, both noted that access to the following must be controlled:

a) Computer sites and mainframes.

b) Terminal sites and terminals.

c) Storage facilities

d) Files and records.

e) System and application programs.

f) Computer output.

g) Telecommunications.

Further, the controls must be applied to people, terminals and programs.

4.3.1. Identification of Individuals

The underlying basis of information processing resources protection is unique identification of an individual. Authorization to access data, obtain information products or use information processing resources is ultimately based on such identification. The techniques available or being actively pursued are quite extensive. They include use of picture badges, magnetic striped credit cards, passwords, fingerprint readers, hand geometry readers, lip print readers, voiceprint recognition equipment, dynamic signature analysis and the like. The identification techniques are applied to supplement or replace human recognition of an individual attempting to gain access to a building, computer room, terminal area, terminal, computer (from a remote site), etc.

Clearly some identification techniques can serve multiple purposes (e.g., magnetic striped cards can be used to control door locks (and as an identification to a computer), while others are limited to a single function (e.g., passwords as a means of identifying an individual to a remote computer or as a method of authenticating access authorization to files).

It is generally true that identification techniques based on something tangible (e.g., a badge or a fingerprint) can be defeated by duplicating the identification. Thus the problem of "breaking security" is transformed into the often simpler task of duplicating or simulating a physical entity.

In general, the methods of automated identification that do not require human perception (magnetic card readers, fingerprint readers, etc.) often involve high implementation costs, so it is often economically feasible to apply them only where there are relatively few points (rooms, terminals, etc.) where such identifications must be made.

The intangible methods of unique identification (passwords and catechetical sequences) have the advantage of not requiring input apparatus but are not as broadly applicable as some of the tangible methods. Primarily because of their low implementation cost and simplicity, intangible identification methods are frequently used in time-shared systems serving a large, frequently changing, geographically dispersed population.

The choice of which methods to use for unique personal identification involves criteria such as user convenience, cost, precision of identification, the number of points where identification must be made, etc. Criteria for evaluating and using such schemes are needed because of the critical role unique identification plays in all aspects of security.

4.3.2. Authorization Mechanisms

Both Mr. Lewis and Mr. Edwards emphasized the need for authorization mechanisms to control access to systems. These mechanisms are often programs that validate a user's (and/or program's or terminal's) right to use a given element being protected (e.g., data, program, terminal, etc.). Mr. Lewis noted that "in practically all cases, the off-the-shelf computers and control programs supplied by the manufacturers have inadequate protection mechanisms for providing controlled access to a computer's assets." Mr. Edwards supported this view and added that most computer systems are sold as complex and expensive do-it-yourself kits.

Examples given of authorization mechanisms included those to validate initial access to a system (e.g., from a terminal), validation of data transmission to a terminal or user (i.e., assuring that both the user and the terminal are "cleared" to receive the data accessed), and validation of access to files (including program files), records and fields.

While many contemporary systems have one or more specific authorization mechanisms (e.g., password validation of terminal users), the mechanisms are not applied uniformly in response to a general security principle. This results in the users having the choice of building their own control programs or modifying that supplied by the vendor in order to obtain the level of controlled access they need. Neither of these alternatives is especially attractive.

Another consequence of the piecemeal "Band-Aid" approach to providing security "features" on contemporary systems is the dispersal of the authorization mechanisms into a variety of control and applications programs. Because controlled access is not a design requirement for the operating system, it is not surprising that current systems have many "holes" caused by incomplete application of the controlled access principle. These "holes" can be exploited by

virtually any programmer to circumvent the security "features" and existing authorization mechanisms to gain unauthorized access to data, programs, or the operating system itself. Of some six (6) to eight (8) penetration exercises run against a variety of machines, all of them achieved undetected unauthorized access to files and programs or supervisory control of the target system.

4.3.3. Technological Needs

Mr. Lewis and Mr. Edwards indicated that in order to meet the stringent requirements of providing data confidentiality (especially in universal access utility systems), it is necessary to have computer systems and control programs (operating systems) built with controlled access or security as a major design goal. In order for users to be able to evaluate the products being offered, it would be necessary for the vendors to supply detailed security specifications that include the (assumed) security perimeter, the external and internal protection mechanisms provided, what they protect from whom, and how the protection is achieved. The goal is to achieve a penetration-proof system with protected authorization mechanisms that permit precise and continuous validation of all access in the system.

It is also necessary to provide systems that can be "certified" to be secure by some independent authority. Drawing on the analogy of the rating of safes and storage containers as being able to resist various attacks (e.g., dial manipulation--20 man-minutes, forced entry--0 man-minutes), Mr. Edwards pointed out that proof (of security) by emphatic assertion will not suffice. It must be possible to convincingly demonstrate that a system is secure under various kinds of attacks. There is also the need to be able to recertify a system in use because of the almost continuous stream of changes that take place in the hardware and software of an operational system.

The primary thrust of the remarks was directed at the requirement to obtain systems that provide protection even against the threats posed by persons with the authorization and capability to produce their own programs (producers). However, even for less demanding environments where protection is required for intruder and consumer threats, much more needs to be done. In particular, the evaluation of already existing technological alternatives for retrofitting existing systems with controlled accessibility mechanisms that are appropriate for the degree of protection required and the potential threat source (intruders, consumers, producers, etc.) is needed now.

4.3.4. Network Security and Cryptography

The controlled access problem is not confined to computer systems alone, as the discussion regarding controlled access and security of the telecommunications networks linking computers and users brought out.

Mr. Charles Joyce, Assistant Director, Office of Telecommunications Policy, in outlining the problem, indicated that the basic network security question to be resolved is what proportion of protection responsibility should the communications subsystem bear.

Dr. Michael Muntner, Director, Advanced Planning and Research Division, Automated Data Management & Telecommunications Service, GSA, noted that virtually all current effort is focused on the terminal end of networks since that is where the bulk of the experience has been. It was his contention that access control requirements are best handled as part of an initial systems design rather than by patches and repairs to systems and networks after the fact. He presented three types of network situations that reflect three different kinds of management control of the resources involved. These were:

a) An integrated system--a single management responsible for both computer systems and telecommunications control.

b) Segregated systems--one management is responsible for only the network and a different management is responsible for the computer (based) resources.

c) Hybrid systems--where one management is responsible for some of the computer (based) resources and the network, while other managements are responsible for the remaining computer (based) resources.

These divided management responsibilities underscore the difficulty of assuring that the security and controlled accessibility of a network of computer (based) resources is properly achieved. It also underscores how the allocation of responsibility for security between the systems and the network can result in each believing the other is (responsible for) taking care of the problem. The basic issues involved in a particular network are:

1. How well the computer systems protect themselves.
2. How deeply can encryption be incorporated into the network.
3. Whether security-related functions can be standardized across all system elements.
4. What records should be kept.

Of these points, 2 and 3 are the most important to networks in general, particularly where the composition of the network is not homogenous in equipment.

Dr. Davis pointed out that cryptographic techniques can be used to protect data during transmission among systems. Cryptographic transformations can be applied to protect data transmitted between a computer and its terminals or other computers. The transformation can be applied to passwords or even data in storage.

Details of cryptographic transformations and their applications have not received wide circulation among civilian (nor most government) information systems developers. As a consequence, users have no basis for evaluating the efficacy of one proposed technique over another. As an example, one manufacturer of commercial scramblers (cryptographic machines) used a simple linear shift register as the generator of the cipher key. Current papers have appeared recently showing how simple it is to "break" such a system with as few as 2N bits of key (where N is the length of the shift register).

In addition to needing an evaluation of the strengths of specific cryptographic techniques, it is also necessary to evaluate whether or not they can meet other protection objectives such as preventing effective alteration or replacement of all or part of the message, or detecting attempts to retransmit previously sent legitimate messages, or denying intrusion on common carrier networks.

The controlled access problems that exist in stand-alone computer systems are quite formidable in their own right. When computers are linked to terminals and each other, there are the considerable additional problems of determining whether attempted user accesses are legitimate and even who is attempting access. Where the interlinking communications system is a switched common carrier (e.g., the telephone network), the opportunities for remote penetration for intercepting data is increased significantly.

The primary needs for network security are criteria that relate costs of data confidentiality to the type of network, inexpensive security techniques (e.g., cryptography) that can be applied to networks of heterogenous equipment, methods of authenticating users and computers which are not susceptible to masquerade, and model secure network designs that clearly identify what protection is provided by the network against specific kinds of threats.

4.4. Computer Security Auditing and Surveillance

A number of speakers mentioned the need for security auditing of information processing systems as a management tool for enforcing data protection policies.

In a discussion of evaluating existing systems, Mr. Robert Abbott, Manager, RISOS Project, Lawrence Livermore Laboratories, focused on the need to audit existing protection mechanisms. In discussing the problems this poses, he cited the lack of data on the experiences of others using contemporary systems and the vast size of current operating systems as discouraging for such analysis.

It was pointed out by Mr. Abbott that pre-use auditing of existing protection mechanisms requires collaborative arrangements with manufacturers that enable the auditors to obtain accurate information about the system under study. The main barrier to such cooperation currently would appear to be the lack of suitable arrangements that protect the proprietary

37-583 O - 74 - pt. 2 - 51

and marketing interests of the manufacturers while providing system auditors with the information needed to evaluate a system in a way that protects its integrity.

In other discussion of auditing the use of systems, several speakers noted the importance of such audits in determining proper use of an information processing resource. Mr. Gould stated that California was developing a master audit package that would measure users' compliance with the security/privacy requirements established for their data. Dr. Branstad also spoke of the use of surveillance and audits to maintain accountability for resource usage and data access.

In the areas of monitoring usage and data access accountability and compliance with protection standards, a major problem is that security auditing is attempted from the operating systems instrumentation for accounting. While much of the same information is needed (e.g., identification of who is using the system) for both purposes, security auditing techniques may require more detailed information on just how a system is being used (e.g., what language processors are used, what physical devices are used, etc.) than that required for accounting purposes alone. An existing technological problem is how to instrument both the hardware and software of a system in such a way that very specific and detailed information on what a user is doing can be selectively recorded without disturbing the operating environment for all others. If this becomes feasible, an effective interface to the systems' management must still be provided which permits specification of the activity to be monitored for a user, device, terminal, line, etc.

V. Costs

5.1. Introduction

The importance of information in our service-oriented society leads to a consideration of the social costs of limiting access to data in the interest of protecting individual privacy and data confidentiality. Since data collection is often required to plan and operate needed service programs, lack of accurate data will either inhibit the development of these programs or raise the costs of implementing and operating them. Either way, there is a cost associated with any "solution" that involves indiscriminate suppression of recordkeeping or makes the operating costs too high by imposing unrealistic standards of data confidentiality and control. These factors are beyond the scope of this summary.

There is a strong indication that the public is willing to pay in some way for privacy and security. Dr. Davis noted that approximately 15% of the telephones in the U.S. have unlisted numbers for which the subscribers pay various rates varying from a $9.00 fixed charge to 50¢ /month. On a less discretionary basis, passengers on national airlines have been paying a surcharge on fares for airport security and anti-hijacking measures. Other widely used services which have a cost component for privacy or security include: recreation, housing, health, education and local (commuting) travel. From these broad-based examples, it is

possible to conclude that the costs for maintaining personal data confidentiality and security in government-operated information systems will be readily borne by the public. As Dr. Davis pointed out, however, the question of cost allocations among the public, industry and government has rarely been addressed. Such studies are needed to form the basis for privacy decisions and the development of appropriate cost allocation schemes.

5.2. Costs of Security

5.2.1. Physical Security

The costs of physical security are more easily identified than the costs for other areas of computer security. Physical security costs include constructing limited access sites for computers and terminals, vaults for tape and disc storage, additional costs for fire detection and suppression and the like. Most of these costs should be allocated to the protection of data processing resources rather than to the protection of data confidentiality. One would expect these measures to be in force independent of the additional need for data confidentiality. Because computers represent an important asset of an organization, they require protection at a level which is at least equivalent to the value of the equipment.

Carefully designed and implemented physical security will provide adequate protection of information processing resources and data bases from intruders. The costs of physical security are a relatively small part of preparing a site for a computer system.

As noted previously, an objective of physical security is to prevent unauthorized individuals from physically accessing a computer system or any of the file media, terminals, etc. As a result, the major additional costs beyond those associated with protection of assets from natural disaster are associated with personnel identification and physical access control. For many systems, a policy of locking the computer room and restricting access to just operations personnel only provides a large increment of security for the system. Mr. Chronis deplored the open showcase kind of installation that results from management being insensitive to the needs of security.

5.2.2. Controlled Accessibility

It is in this area that discussion of costs becomes more emotional than objective. It is sometimes stated that you can design for security and compromise performance or design for performance and compromise security. The problem, of course, is to design for both.

A number of people claim that serious cost penalties are associated with computer security. This was implied in the remarks by Mr. Kenneth Orr who indicated that it was necessary to determine when and how to trade off performance for security. This view comes about in part from acceptance of the fact that access control mechanisms have to be imbedded deeply in the

internal operating systems to provide the computer systems with a large measure of self-protection. The current thinking of the technical community is that the primary way this can be achieved economically is to adapt, modify or change the architecture of the computer system to provide a hardware data access (reference) validation capability in the form of segment tables, descriptors, or address mapping hardware with associated authorization controls. Any attempts to achieve complete data access validation (including that within the operating system) in software alone would indeed raise the execution overhead to an unacceptable level and would also be very costly in terms of additional programming for the reference validation(s). A software-only approach makes it imperative that the software design and implementation be done correctly.

Another aspect of the costs of security was brought out by Mr. Edwards who cited that attempts to "fix" operating systems by patching them are fruitless exercises because the patches are generally repairing a symptom rather than the underlying cause. Because most present efforts at security are patches and additions to a basically unsound foundation, they are fairly easily defeated. Based on his observations of a number of penetration exercises, he estimates the cost of "breaking" a system at roughly 1/10 the cost of creating and installing patched protection mechanisms.

Mr. Abbott indicated a cost of 18 man-months to do a "good integrity study" of a system with up to 6 months of study required to become familiar with the system under investigation. This level of effort is needed to just identify major potential problems.

Still another indication of the cost of security is found in the Air Force Security Technology Planning Study (4) which indicates that the cost of "repairing" a single contemporary system, removing all of the known security deficiencies in the system, is on the order of 2.5 million dollars. As a further indication of the magnitude of these costs, Mr. Gould indicated that the costs attributable to security in the five super centers being developed in California were from $200,000 to $400,000 per center over and above the costs attributable to physical security.

The argument that making systems secure is costly is valid if the systems' architecture does not provide any hardware assistance to enforce the access control protection of the system. In this situation, the cost in performance and other tangible factors that would have to be passed onto the customer is quite high.

There are, however, computer systems with the necessary architectural embellishments that would make it possible to achieve the level of self-protection needed to support access control and authorization mechanisms in a reliable and secure way. Even in these, because security has not been a paramount issue in the design of the operating system, the features most often are haphazardly used. In these kinds of systems, the performance degradation attributable to security is expected to be quite low because the architectural features of utility for security are included for other purposes--primarily for dynamic memory allocation.

Once one has achieved a self-protected system, it is then possible to consider a variety of added authorization mechanisms needed to control the employment of the resources of the system. A self-protected system is not of itself a secure system--rather it is a reliable foundation upon which to build a secure system for given applications.

5.2.3. Communications Safeguards

Communications can be protected either by physically protecting the transmission lines or by using cryptographic devices. Physical protection of the lines is feasible if all remote users are located in the same facility as the computer center. The incremental costs of physical protection of communications lines can be quite small if the overall physical security of a site is good.

The cost of encrypting message traffic among computers and terminals includes the costs of the cryptographic equipment itself and the increased administrative costs of protecting the keying information. It is necessary to physically protect the cryptographic device from unauthorized access or tampering as well, but this cost may be minimal if the remote site already has adequate physical protection.

Typical commercially available cryptographic devices or scramblers cost in the range of $2000 to $5000 per unit, with discounts usually available for quantity orders. Where only a few lines are protected in this way, there is no special problem encountered. However, when it is necessary to protect a large number of lines, then the costs of having a scrambler at both ends of every link become significant. None of the manufacturers of this equipment have developed multiplexed cryptographic techniques for this kind of application. Scramblers based on simple principles can sometimes be simulated in a computer, thus achieving the desired multiplexing. However, this appears to be possible only for those scramblers whose principle is also susceptible to simple analysis and exploitation.

Basically, the communications protection costs can be easily ascertained if the need is recognized.

5.2.4. Costs of Not Providing Technological Safeguards

As the need for data security is recognized and legislation is enacted to protect data confidentiality, governmental agencies will be faced with establishing stringent data-handling procedures to protect this data. Without technological safeguards which can provide this protection, other "stop-gap" measures must be used. The costs resulting from using these measures on contemporary systems are:

- inefficient utilization of existing hardware and personnel, or the acquisition of extra hardware and personnel to maintain separation of protected data

- loss of information accuracy, timeliness and completeness resulting from reduced data sharing and inadequate data correlation brought about by having to maintain separation of protected data from other data.

Specific operational procedures being used and the cost incurred for providing security and data confidentiality for highly sensitive or valuable data include:

- separate computers for separate applications to achieve isolation, when combined operation on a single machine would otherwise significantly reduce costs;
- sharing of a computer by several applications sequentially instead of concurrently, resulting in costly change-over procedures;
- scheduling applications involving protected data at times when time-sharing terminals are disconnected;
- restricting capabilities of users at remote terminals.

These practices require substantially more equipment and personnel than would be required for operation on self-protecting resource-sharing systems. Not only are the direct equipment and people costs increased, but so are the costs resulting from reduced operational effectiveness. It is estimated that the increased costs resulting from these practices range between 10% and 100% of the costs of operating an installation, with an average cost estimate of 40%.

VI. Action Plans

6.1. Introduction

Progress toward resolving the governmental needs and problems identified during this Conference requires the coordinated efforts of the nation's legislatures, government management, the service industries, and the automation industry. A realistic approach to providing solutions could consist of parallel and coordinated efforts directed toward:

- Achieving a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.
- Establishing uniform management and technical procedures and guidelines for the effective application of security measures.
- Innovative applications of existing technology to enhance security mechanisms and techniques.
- Research and development where the technology needed to eliminate serious security deficiencies does not exist.
- Studying and allocating costs of confidentiality and security in automated information systems.

6.2. Cohesive Legislation

A national legislative conference called for the purpose of considering the adoption of uniform legislative policies, definitions, requirements and penalties would represent a significant contribution to assuring the effective implementation of laws that are enacted.

Specifically needed are definitions of the rights to be accorded to individuals in the collection, use, and dissemination of personal data and the disclosure of information to the individual for purposes of verification. The recommendations of the HEW Advisory Committee could serve as a point of departure for such a conference (see Appendix A). An expected outcome of the conference would be model Federal, State, and local legislation for addressing the privacy problem. A number of such models are in existence. These could be considered and either recommended or modified as required.

In formulating model legislation or specific proposals, it is essential that the legislative branch at all levels of government have the advice of the technological community to assess the technical feasibility and impact of proposals designed to protect data confidentiality. In addition to the expertise of the appropriate government technical organizations, the computer technical societies, such as the Association for Computing Machinery and the Computer Society of IEEE, should make their resources available to interested legislative committees.

6.3. Uniform Management and Operating Procedures

Cooperative efforts among government agencies, professional societies, computer industry and private sector groups, such as the American Banking Association and the American National Standards Institute, can result in the early agreement, documentation, and widespread distribution and implementation of useful management and operating procedures.

In particular, efforts should be directed toward determining levels of data confidentiality required for the protection of privacy rights and their impact upon technological support requirements. Since these levels can be expected to vary among special user communities, such as health, law enforcement or credit services, initiatives can be exercised by these communities in cooperation with the computer and information technologies.

Of broader and more common application are techniques for such activities as assessing risks, determining threats and threat sources, evaluating alternative security measures, auditing and physical security. Some of these techniques already exist and could be readily documented for wide dissemination and use. As an example, the National Bureau of Standards is developing physical security guidelines which will be made available through public distribution channels. Other organizations with documented techniques could offer them for use elsewhere or, working jointly, could speed up development of techniques which are not now available.

Models of computer system and data protection measures that could be used against various threats would be extremely helpful in providing management with ready-made designs for the operation of secure automated data systems that could be adapted to meet local needs.

6.4. Research and Development

Interaction among government agencies, other user communities, and industry groups can lead to general agreement on significant needs and problems which cannot be satisfied by existing science and technology. Research and development efforts to fill these gaps could proceed on a coordinated but independent basis.

This Conference has initially identified several such needs. Among these is a need for self-protected computer systems. While techniques for controlled accessibility exist for systems which are not programmed by their users, little is being done to generate self-protected systems as a base for resource-shared systems which are secure against threats by producers (where programming access is provided to some or all users). The focus of ongoing efforts is to develop secure advanced time-sharing systems supporting on-line programming, extensive program-sharing facilities and the like (such as the Air Force project to develop a certifiably secure system and a multi-mini computer system, such as that being developed at the University of California, Berkeley.)

In addition to this important work, there is a need to develop self-protected systems on other suitable equipment. In order to accomplish this, it is necessary to define uniform self-protection requirements and to develop models of controlled accessibility that are based on other modes of computing, such as multiprogrammed use of systems with data file sharing in production environments.

Secure operating systems are those with access authorization mechanisms which use the system's self-protection mechanisms to enforce the access limitations of a programming user (producer). In such a system both the self-protection and access-authorization mechanisms must be self-contained and certifiable. One expression of these concepts is found in the Air Force Computer Security Technology Planning Study. It postulates systems in which all references of any program to any other program, data, or peripheral device are validated during execution against a list of authorized types of reference based on user and/or program function. This idea is called a reference monitor concept and is to be realized in a combination of hardware and software called a reference validation mechanism.

It is the efficiency consequences of the requirement for validating each reference of an executing program that leads to a search for hardware techniques to perform this function. For this reason, descriptors or address mapping tables that include reference-type checking appear attractive for developing secure systems.

The software components of a reference validation mechanism include the processing of authorized references for each user/program function to set values in the tables/descriptors used in reference checking, software that provides for the administration of the authorizations for individual users, and software that deals with attempted violations of authorized access.

Another need for further research and development relates to network security. The outstanding needs of network security are not generally understood by either users or the technical community at large. Not only is the security of information processing systems connected via a network at stake; but the network, itself, becomes an object of security interest. A coordinated research program to provide secure network models which can be used to measure and evaluate costs, protection, and service would help designers to decide where to allocate any security-related functions to the network and, if so, which ones (e.g., user identification, authorization checks).

Finally, the inability to positively and uniquely identify individuals who are authorized to gain access to computer systems and data remains a basic obstacle to computer security. Further research and development of identification techniques, together with network security and self-protected systems, represents an initial set of requirements around which, by common consensus, a coordinated program can be pursued.

6.5. Innovative Applications of Technology

Innovative applications of existing technology can produce improvements in the capability of currently available systems to protect data. Cooperative efforts among users, user communities and the computer industry to develop and stimulate new ideas and to publicize successful experiences can make a positive near-term impact upon security effectiveness.

Two such possiblities were identified at this Conference. The first relates to the retrofitting of existing systems to satisfy new security requirements.

On most systems, for example, it would be fairly easy to validate a program's authority for initial access (e.g., OPEN) to a given file or a user's authority to call for the execution of a given program. Because these validation functions would occur only once per job, they are not too costly to consider using and would provide at least a first level of controlled accessibility for a system. It would be possible but more difficult to provide validation of authority to access specific records of a file since it would require a representation of the access privileges accorded to the use of a file (e.g., records could be individually tagged for reading only) or to each record by a label which shows in some meaningful way the kinds of restrictions on its use.

Where the individual making the access is a consumer only, record access validation can be still relatively simple. However, the complexity increases if record access validation is applied to producers who can generally request any processing action on a record (e.g., read, write, delete) and whose authority to access a record has to be determined in the specific context of the request.

While centralized authorization mechanisms will not solve all possible controlled accessibility problems for any particular system, they will provide greater data security on systems than is presently available and in many cases will be adequate in the short run.

A second possibility for the innovative application of existing technology involves the use of cryptographic devices and data encryption techniques. The National Bureau of Standards is currently engaged in making available encryption algorithms to provide a way for civilian agencies of government to protect the contents of data during storage and transmission. Related to the use of these techniques is the need for low-cost effective cryptographic devices that can be used to protect data confidentiality and integrity in systems using telecommunications. With the availability of self-protected systems, programmed encryption techniques become viable as a means of protecting data on physical storage media or between devices with computational capability. However, such techniques impose additional burdens of key management that need cost-effective resolution. Therefore, development of techniques for efficient key management are also needed.

6.6. Cost Allocations

A study of the costs of data confidentiality and security in automated systems is essential in creating an understanding for making public choices about the privacy needs of individuals and for allocating the costs among the suppliers, the user communities, the public and the government. Costs must be identified and acceptable concepts developed for cost allocations schemes. Since these will undoubtedly vary among such service activities as government, banking, credit and medicine, appropriate studies might logically be organized on this basis and participated in by management, economists, and technologists.

Appendix A

CONFERENCE PROGRAM

Monday, November 19, 1973

8:15 a.m. Conference Registration

9:30 CONFERENCE INTRODUCTION

Welcome: Dr. Richard W. Roberts, Director, National Bureau of Standards

Keynote Remarks: Honorable John K. Tabor, Under Secretary of Commerce

The Congressional Interest: Honorable Jack Brooks, Chairman, Government Activities Subcommittee, Committee on Government Operations, House of Representatives

A Statement of the Problem: Dr. Ruth M. Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards

10:30 - 10:45 Break

10:45 - 1:00 SAFEGUARDING PRIVACY
Mr. David B. H. Martin, Session Chairman
Special Assistant to the Secretary
Health, Education and Welfare

Governmental Systems with a Need for Privacy Protection

Federal: Mr. George Hall, Acting Assistant Administrator, Law Enforcement Assistant Administration, Department of Justice

Municipal: Mr. Andrews Atkinson, Superintendent, Cincinnati/Hamilton County Regional Computer Center

Issues and Requirement for Privacy Safeguards

Professor James Rule
State University of New York

A California Solution

Mr. Kent Gould, Chief, EDP Control & Development, Department of Finance, State of California

1:00 - 2:15 Lunch

2:15 - 5:15 CONTROLLING ACCESS TO SYSTEMS AND DATA
Mr. Walter W. Haase, Session Chairman
Deputy Assistant Director, Information Systems,
Office of Management and Budget

The Need and Significance of Controlled Accessibility

Dr. Dennis Branstad, Project Leader, Computer Security, National Bureau of Standards

Governmental Systems with a Need to Control Access

Federal: Dr. Robert Laur, Acting Director, Office of Policy Development and Planning, Health, Education and Welfare

State: Mr. Jerry Hammett, Deputy Director, Department of Finance, State of Ohio

Congress: Mr. Robert Chartrand, Science Policy Research Division, Congressional Research Service, Library of Congress

Providing for System, Program and Data Integrity

Mr. Howard E. Lewis, Jr., Manager, Data Management Programs, Atomic Energy Commission

Managing Computer Operations

Mr. Robert Caravella, Management Information Division, Department of Finance, State of Illinois

Tuesday, November 20, 1973

8:15 a.m. Conference Registration

9:00 - 10:30 CONTROLLING ACCESS TO SYSTEMS AND DATA (cont'd.)
Mr. Charles Joyce, Session Chairman
Assistant Director, Office of Telecommunications Policy

Controlling Access to Local Computer Systems

Mr. Daniel J. Edwards, Research Engineer, National Security Agency

Controlling Access to Computer Networks

Dr. Michael Muntner, Director, Advanced Planning and Research Division, Automated Data Management & Telecommunications Service, General Services Administration

10:30 - 10:45 Break

10:45 - 11:30	INTERNATIONAL ACTIVITIES RELATED TO PRIVACY Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University
11:30 - 1:00	REQUIREMENTS FOR PHYSICAL SECURITY Mr. Ike Friedlander, Session Chairman Executive Director, Public Buildings Service General Services Administration
	Records and Personnel Management
	Dr. Walter E. Simonson, Associate Director of Electronic Data Processing, Bureau of the Census
	Protecting Against Environmental and Other Hazards
	Mr. Nicholas A. Chronis, Chief, Data Processing Computer Center, Civil Service Commission
1:00 - 2:15	Lunch
2:15 - 3:45	ASSESSING SECURITY RISKS AND COSTS OF PROTECTION Mr. Carl Vorlander, Session Chairman Executive Director, National Association for State Information Systems
	Auditing Existing Protective Measures
	Mr. Robert P. Abbott, Manager, RISOS Project, Lawrence Livermore Laboratories
	Management Evaluation of Needs, Benefits and Costs of Security Protection
	Mr. Ken T. Orr Topeka, Kansas

Appendix B

Publications/References Cited at the Conference

1. "Records, Computers and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare, July 1973, U.S. Government Printing Office (Stock No. 1700-00116), Washington, D.C. 20401, Price $2.35, postpaid.

2. Federal Fire Council Publication RP-1, "Fire Protection for Essential Electronic Equipment," available from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22151, under document number AD-692-662. Price $6.00.

3. DOD Directive 5200.28 and appendix 5200.28 M. Office of the Secretary of Defense, the Pentagon, Washington, D.C. 20301.

4. "Computer Security Technology Planning Study," October 1972, Electronic Systems Division, L.G. Hanscom Field, Bedford, Massachusetts 01730, ESD-7R-51, Vol. I and II.

5. Report of GUIDE Subcommittee on Security Requirements.

6. Project SEARCH Security and Privacy Publications available from: Project SEARCH, CCTRF, 1927 13th Street, Sacramento, California 95814.

7. GMIS Project 73 publication: An Administrative Guideline for Security and Confidentiality in State and Local Government Data Centers, GMIS, 138 East Court Street, Cincinnati, Ohio 45202, price $25.00.

Appendix C

Preview of Conference on Privacy and Computer Security
National Bureau of Standards, Gaithersburg, Maryland
March 4-5, 1974

This Conference is planned as a sequel to the November 1973 Conference to continue the dialog and interaction among government, industry and public interest groups that is needed for effective resolution of the privacy and computer security issues.

More specifically, this Conference provides an opportunity for the computer industry and other groups in the public and private sectors to present solutions, ideas, and approaches for dealing with the governmental needs and problems outlined in this Conference Report. The suggestions may include legislative, technological or managerial measures, and may focus on existing state-of-the-art techniques, advanced methodologies currently under development or promising research interests of a longer range nature.

Participants in the program will include persons from:

- The Congress
- State legislatures
- Individual computer companies and consulting organizations
- Professional organizations
- Academia

Attendance at the Conference is open to all interested persons, including management and technical personnel from Federal, State, and local governments, the computer industry, public interest groups, professional associations, academia and privacy and security experts.

Further information may be obtained from the Conference office:

NBS Privacy and Computer Security Conference
Administration Building, Room 209A
National Bureau of Standards
Washington, D.C. 20234

Phone: (301) 921-3195

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS TN-809	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE
Government Looks at Privacy and Security in Computer Systems. Summary of a Conference held at the National Bureau of Standards, Gaithersburg, Maryland, November 19-20, 1973

5. Publication Date: *February 1974*

6. Performing Organization Code

7. AUTHOR(S): *Clark R. Renninger and Dennis K. Branstad, Editors*

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS
NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.: *640.1110*

11. Contract/Grant No.: --

12. Sponsoring Organization Name and Complete Address (Street, City, State, ZIP)
Same as No. 9

13. Type of Report & Period Covered: *Final*

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)

This publication summarizes the proceedings of a conference held for the purpose of highlighting the needs and problems of Federal, State and local government in safeguarding individual privacy and protecting confidential data contained in computer systems from loss or misuse. The Conference was held at the National Bureau of Standards on November 19-20, 1973.

The origin of governmental problems is discussed in the context of the public's concern for privacy arising out of computer-based recordkeeping, the diverse legislative actions how being taken to safeguard privacy, the threats to the security of computer-based information systems and the technological problems associated with protecting against such threats. Useful distinctions are drawn between privacy, confidentiality and security to clarify the issues and allocate responsibilities for solving the problem among lawmakers, technologists and management.

Major needs are described. These include the need for cohesive Federal, State and local legislation, technological guidelines and standards for assuring uniform compliance with legislative requirements; management guidelines for identifying and evaluating threats to security; and improved technological mechanisms for controlling access to computer systems and networks. Cost implications of providing security measures are discussed.

17. KEY WORDS (six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)
Computer systems, privacy and security; confidentiality; privacy; security.

18. AVAILABILITY
[X] Unlimited
[ ] For Official Distribution. Do Not Release to NTIS
[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13
[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT): UNCLASSIFIED

21. NO. OF PAGES: 47

20. SECURITY CLASS (THIS PAGE): UNCLASSIFIED

22. Price: 85 cents

USCOMM-DC 29042-P74

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. Comprehensive scientific papers give complete details of the work, including laboratory data, experimental procedures, and theoretical and mathematical analyses. Illustrated with photographs, drawings, and charts. Includes listings of other NBS papers as issued.

Published in two sections, available separately:

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS, NBS

The best single source of information concerning the Bureau's measurement, research, developmental, cooperative, and publication activities, this monthly publication is designed for the layman and also for the industry-oriented individual whose daily work involves intimate contact with science and technology *—for engineers, chemists, physicists, research managers, product-development managers, and company executives.* Annual subscription: Domestic, $6.50; Foreign, $8.25.

NONPERIODICALS

Applied Mathematics Series. Mathematical tables, manuals, and studies.

Building Science Series. Research results, test methods, and performance criteria of building materials, components, systems, and structures.

Handbooks. Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications. Proceedings of NBS conferences, bibliographies, annual reports, wall charts, pamphlets, etc.

Monographs. Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

National Standard Reference Data Series. NSRDS provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated.

Product Standards. Provide requirements for sizes, types, quality, and methods for testing various industrial products. These standards are developed cooperatively with interested Government and industry groups and provide the basis for common understanding of product characteristics for both buyers and sellers. Their use is voluntary.

Technical Notes. This series consists of communications and reports (covering both other-agency and NBS-sponsored work) of limited or transitory interest.

Federal Information Processing Standards Publications. This series is the official publication within the Federal Government for information on standards adopted and promulgated under the Public Law 89–306, and Bureau of the Budget Circular A–86 entitled, Standardization of Data Elements and Codes in Data Systems.

Consumer Information Series. Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service (Publications and Reports of Interest in Cryogenics). A literature survey issued weekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to the U.S. Department of Commerce, National Technical Information Service, Springfield, Va. 22151.

Electromagnetic Metrology Current Awareness Service (Abstracts of Selected Articles on Measurement Techniques and Standards of Electromagnetic Quantities from D-C to Millimeter-Wave Frequencies). Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to the Electromagnetic Metrology Information Center, Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

Order NBS publications (except Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

37-583 O - 74 - pt. 2 - 52

CONTROLLING ACCESS TO YOUR COMPUTER MAY BE YOUR BEST SELLING POINT—AFTER-DINNER ADDRESS TO THE WASHINGTON CHAPTER, DATA PROCESSING MANAGEMENT ASSOCIATION, MAY 15, 1974

By Dr. Ruth M. Davis, Director, Institute for Computer Sciences and Technology
National Bureau of Standards

The days of getting "brownie points" for building bigger and faster systems for handling personal information are at an end. They are being washed away by a great tidal wave of national concern for individual privacy and a rising demand for greater protection of the personal data in our computer systems.

I suspect that we are entering a time when the real technological heroes will be those who devise more effective,, foolproof ways to control access to computer systems and protect the confidentiality of the information they store and process. Even greater recognition will probably go to the managers and executives who find that they really don't need to collect and maintain cradle-to-grave information about every citizen.

It was not an idle exercise, therefore, when I selected as my topic tonight the theme that Controlling Access to Your Computer May Be Your Best Selling Point.

In the face of mounting privacy pressures, we must not allow ourselves to be stamped into scrapping our computers or adopting repressive measures that will constrain the versatility of the computer in doing beneficial work. Computer technology is neutral; the computer itself is not maleficent—people are. Our task in protecting privacy, therefore, is one of building effective barriers between the computer and the maleficent individual who would use it to deprive others of their privacy rights, to steal property or otherwise violate the law. Just as we try to keep firearms out of the hands of criminals, so must we keep the computer out of the hands of those who would use it to steal information or embezzle funds. I do hope, however, that we are a great deal more successful in separating the criminal from the computer than we have been in keeping him away from guns.

After a quarter century of using computers, why should computer security suddenly become so important? I believe the answer to this question is made up of three interlocking parts—the growing incidence of computer-assisted crime, the explosive growth in the use of computer terminals, and a generally heightened level of sensitivity on the part of the overall population.

The damages resulting from detected computer-assisted rip-offs have reached alarming proportions. Two examples will illustrate this point. A head teller of the Union Dime Savings Bank in New York City was indicted last year for embezzling over $1.5 million by using a terminal to manipulate accounts in a central computer. A bank vice president and an employee of a discount chain embezzled $6.8 million during the changeover to a computer system. Not all detected computer-assisted crime is on this level but, of course, we don't know what may still be undetected.

In its November 1973 report on Computer Abuse, the Stanford Research Institute has recorded 148 cases of computer abuse that have occurred over the last decade. Ninety-nine of these cases involved financial fraud or the theft of information, property or money; 26 involved vandalism and 23 involved the unauthorized use or sale of services. The cases were spread over a wide spectrum of activities including banking, insurance, manufacturing, computer services, education, welfare, and civil service. Some of the more interesting of these cases involved the theft or misuse of information. For example:

A programmer was accused of bigotry because he programmed a computer to eliminate black candidates in screening and selecting new employees.

An employee destroyed on-line data files after being given notice of termination of employment.

3 million customer addresses were stolen by three night-shift computer operators in a publishing firm.

A computer service firm used a registered voters address list for commercial purposes.

A policeman is alleged to have obtained from the FBI National Crime Information Center the dossier of a man involved in a transaction with the policeman's brother-in-law.

Several programmers stole information from a payroll system and sold it to an insurance company agent.

A political candidate is alleged to have requisitioned a mailing list of state civil service employees for use in political campaigning.

These few cases illustrate some of the ways personal data can be misused. They underscore the importance of the basic thrust of some of the privacy legislation now before the Congress. These examples also illustrate the diversity of computer-assisted crime and, in sketchy fashion, indicate how extremely difficult it will be to curb such abuse without major improvement in computer security on a broad front. Technological methods to control computer abuse are necessary, but not sufficient. Legal and social remedies must also be considered.

Unfortunately, we can expect computer-assisted crime to increase in the future as computers and data communications push even further into the functioning of society and industry. The computer terminal, if it isn't already, will undoubtedly become the chief crow-bar for breaking into computer systems and plundering their contents. At the present rate of growth, there should soon be enough terminals in use to make it relatively easy for computer burglars to gain access to one for a while. Until relatively recently, users generally bought only a few terminals at a time: now, however, with the advent of the electronic point-of-sale terminal and bank transaction devices, users are buying them in lots of several thousand units each. Some of the large department store chains like Montgomery Ward and J. C. Penney have placed orders for 15,000 or more terminals at a time.

The computer terminal market is one of the fastest growing sectors of the computer industry. The number of general purpose terminals in use is expected to increase from 280,000 in 1972 to nearly a million by 1977. Special application terminals, including point-of-sale and banking devices, will grow at an even more spectacular rate. In fact, the general merchandise industry expects to have in excess of 200,000 POS terminals installed in its department stores by the end of 1974. Supermarkets are projected to account for another 100,000 automated checkstand terminals by 1980.

The proliferation of computer terminals is making it possible for more people to have access to computer systems and data banks. At the same time, they are broadening the spectrum of business activities that are dependent on computer systems. These developments, in turn, are significantly escalating both the opportunity and the incentive for computer-assisted crime through the unauthorized accessing of computers and the misuse of the information they contain.

The reported cases of computer crime notwithstanding, one might wonder how really widespread is the concern over privacy and computer security. I think there is convincing evidence that the concern is really and generally widespread. For example, the National Retail Merchants Association which represents more than 30,000 department, variety and specialty stores with annual sales exceeding $50 billion recently established a special task force to handle the computer security problems associated with the mounting use of electronic point-of-sale terminals in the retail industry. A further measure of the concern can be seen in our own November 1973 computer security and privacy conferences which was attended by 510 people representing 46 Federal agencies, 37 State and local governments, and 41 professional associations, universities and public interest groups.

The general mood of the country is also an important factor in general concern over privacy. Congressman Moorhead, Chairman of the House Subcommittee on Foreign Operations and Government Information, recently said:

> . . . Two of the major issues in Government today are the lack of credibility and invasion of privacy. Our citizens are beginning to question whether our Government tells the truth, and perhaps even more ominous, are beginning to fear their own Government. These developments constitute an evil trend which the people of any free society can only find intolerable.

Congressman Rhodes, speaking in support of the Goldwater bill, further elaborated on the citizens' concern over privacy, He said:

> There are, at present, 54 nationwide organizations which have 750 data banks containing extensive information on 130 million citizens. These dossiers are, in too many instances, readily available to persons, business firms of other agencies . . . Like it or not, we have become a nation of snoopers. Data is now collected by various sources and can be collated from these numerous sources and put together in a dossier that represents an overt intrusion into the privacy of individuals. In most cases, the victim is unaware that his neighbors, fellow workers or possibly even his laundry man have been queried about his habits, his occupation or his home.

The Executive Branch of the Federal government has, of course, been concerned for a long time with the protection of information. Until quite recently, this concern has been concentrated in the intelligence community and certain

security agencies with very little attention being given to the civil agencies. The National Bureau of Standards initiated its computer security program about three years ago. This program was designed to serve the needs of the civil sector and, wherever appropriate, to provide a technological bridge to the national security community in order to facilitate the use of security technology already developed for national defense.

The latest Executive Branch action took place on February 23, 1974, when the President announced the establishment of a Domestic Council Committee on the Right of Privacy. The Committee, headed by the Vice President, was made up of 5 Cabinet officers plus the Chairman of the Civil Service Commission, the Director of the Office of Consumer Affairs, the Director of the Office of Telecommunications Policy, and the Director of the Office of Management and Budget. The Committee was charged with exploring the ways that the Government collects, stores and uses information and recommending executive and legislative actions to insure that individual privacy is protected.

To date, the Privacy Committee has set up on the order of ten projects to explore specific subjects related to the question of privacy. A task force has been established to handle each project. In each case, the task force is headed by a designated lead agency and makes use of representatives from the Federal agencies that have a unique responsibility or technical competence relative to the task force's line of investigation. The Privacy Committee and its task forces are working hard to prepare and submit reports within the four month deadline set by the President.

The more far reaching privacy actions are taking shape in the Congress where there appears to be growing bipartisan support for some form of privacy legislation aimed specifically at protecting the confidentiality of personal information in computer data banks. Although several legislative proposals have been introduced, those sponsored by Congressman Goldwater of California and Congressman Koch of New York appear to be receiving most attention.

Congressman Goldwater introduced his first bill (HR 10042) on September 5, 1973; its purpose was to provide standards of fair information practices. Congressman Koch first introduced his bill on January 22, 1974 the purpose of which was to provide that persons be apprised of records concerning them which are maintained by Government agencies.

On April 30, 1974, Mr. Goldwater and Mr. Koch jointly introduced HR 14493. The purpose of this bill is to "protect the right of privacy of individuals concerning whom identifiable information is recorded by the Federal government by enacting principles to govern Federal agency information practices". The resolution is called the "Right to Privacy Act".

Because HR 14493 appears to be the focus of legislative attention in the privacy area, it is worthwhile to review briefly some of the bill's major provisions.

First, the bill specifies ten principles of information practice. The major principles are—

There should be no personal information system whose existence is secret, and the Federal government should not collect personal information except as authorized by laws.

Information should be relevant to the purpose for which it was collected, and should not be obtained by fraudulent or unfair means.

Information should not be used unless it is accurate and current.

The individual should be able to learn what information is stored about him and how it is used and disseminated; moreover, he should be able to correct erroneous information.

Federal agencies should prevent the misuse of information. The administrative procedures set by the bill require, among other things that the holding agency keep a list of all persons having regular access to personal information, and maintain a record of every access to personal information by persons or organizations not having regular access authority—such a record to include the identity of the accessor and the purpose of the access. These provisions are particularly important because of the impact they would have on information system operating costs and procedures. While we don't have hard impact data, it is reasonable to assume that for some personal data files the maintenance of access records alone could double the file size within a few years. This means more storage equipment and, depending upon the specific circumstances, could degrade overall system response time.

Another important feature of the bill is the requirement that each agency give annual public notice of the existence and character of each personal information system it maintains.

The heart of the bill is the section on the rights of data subjects or the people about whom information is maintained. Under this section, the data subject has the right to inspect all information about himself, to learn the sources of the information, and to know the identity of all persons and organizations that have had access to the data and for what purpose. The data subject also has the right to challenge, correct or explain information about himself in the information system. In case there is an unresolved dispute over the accuracy of information, the data subject may file a 200 word statement of his position; this statement must be supplied with any further release of the disputed information. If a dispute remains unresolved, the data subject may request the assistance of the Federal Privacy Board.

The bill also specifies that data subjects of archival-type inactive files, records, or reports must be notified by mail of any reactivation, accessing or reaccessing of the files.

Finally, the bill proposes the establishment of a Federal Privacy Board appointed by the President with the consent of the Senate. The Board would have several important functions:

Publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system maintained by a Federal agency.

Make rules to assure compliance with the Right to Privacy Act.

Perform or cause to be performed such research activities as may be necessary to implement the act and assist Federal agencies.

Order Federal agencies found in violation of the act to cease and desist; such orders may be enforced in a civil action in the appropriate U.S. district court.

Hold open, public hearings on petitions for exceptions or exemptions from the act, and make recommendations to Congress. In addition to the privacy actions underway in the Federal government, I would like to acknowledge, of course, that private groups are also on the move. I note with pleasure Donn Sanford's recent announcement that DPMA Executive Council has adopted a standard of ethical professional conduct in the area of privacy of individual records in data bank systems.

I would like to turn now to the technological imperatives of computer security. What can be done or what must be done technologically and procedurally to control access to computer system and to protect the information they contain? I believe the technologist must be doing two things rather immediately:

To the extent possible, we must accurately represent computer security technology to our legislators to insure that whatever legislation is enacted can be effectively implemented within the technology.

We must vigorously exploit the technology in highly innovative ways to develop and apply the controls that are needed to safeguard our computers and the information they contain or handle.

At the Federal level, at least, we have already begun the process of providing technological information to the legislators. The National Bureau of Standards is playing a key role in this process and is drawing on the results of the computer security program it started some three years ago. While we certainly aren't the only ones representing the technology to the Congress, the Bureau's input is uniquely objective and carries with it the imprimatur of a laboratory that for more than 70 years has served the country fairly and competently. Our actions bear the imprint of our strong conviction that resolution of the security and privacy problem requires the coordinated, in-step efforts of the judiciary, the legislature, Federal, State and local management, information service industries, and the automation and information technology industries.

In this area, there are three terms, i.e. privacy, confidentiality and security, that must be understood. Stated as briefly as possible—

Privacy applies to individual;

Confidentiality applies to data; and

Security is the protection of hardware, software and data.

I would like to concentrate now on just the security aspect. Security has three main components: physical security, data security and controlled accessibility.

Although physical security is a concept with which most of us are familiar, there is a lot more to it than simply putting a lock on the computer room door. The importance of physical security is best illustrated by some examples of what has happened when security has been lax:

Two assassination attempts with handguns have been made on computers—one in Washington State and one in South Africa; in both cases, the shots were non-fatal.

Several computer facilities, including the now famous computer at the University of Wisconsin have been bombed.

The CPU of another computer was done-in by an overdose of acid and a set of wire snips.

Two enterprising burglars each stole a complete computer: the first made off with a completely assembled minicomputer, and the second stole all the components, a piece at a time, and assembled them at home.

University students in Massachusetts captured a computer center and used it to extort concessions from the administration.

Students at New York University kidnapped an AEC computer and held it for $100,000 ransom.

These kinds of acts are preventable if management is alert to the potential of their occurrence and puts in place an effective combination of physical security measures and administrative procedures. The National Bureau of Standards believes that physical security is the first line of defense and is the area where effective barriers can be erected most easily and quickly. Accordingly, NBS has devoted a significant effort to the physical security area. We currently have in printing a physical security handbook for ADP installation managers. The handbook will be published as Federal Information Processing Standards Publication 31 (Guidelines for Automatic Data Processing Physical Security and Risk Management).

The handbook provides managers a comprehensive set of guidelines to follow in assessing his physical security risks and then planning and implementing security barriers and procedures to counter those risks. In addition to security analysis and physical protection, it includes guidelines on anticipating natural disasters, supporting utilities, system reliability, internal controls, contingency planning, and, most importantly, internal audits to determine how well the physical security system is working.

Computer security will undoubtedly be expensive, whether we are retrofitting existing systems or buying new systems with built-in security features. For this reason, it is imperative that the knowledge of computer security not be a tightly held secret of the computer center manager; executives and other senior managers in the organization must also have an appreciation of the subject. NBS has already moved to fill this need by developing an Executive Guide to Computer Security, a publication that is now in printing.

The Executive Guide is aimed specifically at telling the executive what computer security is and why it is important; describing the real world situation as it exists today; pointing out the vulnerabilities of computers; and discussing both the technical and management solutions to the problem.

If past patterns hold, we can expect to be inundated soon with a variety of physical security devices—some may even work. We are already beginning to see some evidence of this phenomenon; however, in fairness to the manufacturers we haven't yet had the opportunity to evaluate the effectiveness of some of the new products.

Positive identification of an individual plays an important part in physical security. We've all heard the claims for one device or another. The picture badge had its day but it allowed an assortment of "apes and long-dead archvillians" to get into some mighty sensitive areas. The identification card with the magnetic stripe seemed like a good idea until we discovered that the magnetic stripe would be copied with nothing more sophisticated than a moderately hot iron.

The search for a foolproof identification device to guard the doors to computer rooms and control access to computers via terminals is still going on. One relatively new device is one that uses hand geometry as the basis for personal identification. The device measures the geometry of the hand, encodes the measurements and either stores the measurement data in a computer or writes them on a magentic stripe card. When the subject wants to enter the secure area, he places his hand on the device and his geometry is compared with the stored or recorded data. The supporters of this process claim that there is sufficient uniqueness of each person's hand geometry to make consistently accurate positive identifications. We have not yet seen the rigorous proof to support this claim.

Fingerprints have been the accepted form of positive identification for a long time but the vat of ink, cleaning fluid and paper towels associated with fingerprinting detract from their utility as a means of controlling access to protected areas. This situation may be changing now with some of the new efforts to develop "instant" fingerprint identification devices. Several such devices are under development and some have reportedly reached the prototype stage. The reassuring feature of this approach is the great amount of both theoretical and empirical data we have about fingerprints as a means of identification.

A third form of automatically measured biometric data for personal identification is the voiceprint. Devices in this area perform a spectrum analysis of a segment of speech and then plots frequency versus time versus energy intensity. These data are then used as the baseline for comparing voice prints for identification purposes. These devices are reportedly only about 90 percent accurate in comparing two voice prints and determining whether they came from the same speaker.

During the first days of World War II, the world learned that an army encapsulated in a steel and concrete Maginot Line was no match for a highly mobile armored force. We certainly don't want to build a second generation Maginot Line around our computer facilities and find ourselves outflanked by blitzkrieging attackers who never come into the line of fire of our physical security guns. We really need an interlocking system of defenses and barriers that can resist the most resourceful attacker and deny him ultimate access to the data.

If an attacker successfully penetrates our barriers and does get to the data, we would like to be able to have the data in a form that makes the data useless to the attacker. We can do this by encrypting the data, that is, putting the data into a code.

We can encode data by using a encryption algorithm that transforms the plain text characters into coded character representations. We can decode the data by using the encryption algorithm in "reverse", i.e., removing the code and recovering plain text. Encryption schemes generally are based on mathematical formulas and random number generators.

Encryption is a solution to the data security problem. We can use encryption to encode data that is resident in the computer or in transit over data transmission lines. If we use encryption, we must implement very effective means for protecting the keys that control the encryption and decryption processes.

Controlled accessibility is the third part of computer security. It consists of the technological measures of hardware and software available in a computer system to protect data.

I think it is clear that in order to effectively protect personal data in computer systems we will have to mount a superbly synchronized and integrated effort on the several fronts of technology, legislation, and management. The skeletal structure of such an effort is already in place. The greater emphasis now is on technology and legislation. We need to do more to speed up actions in the mangement area. I urge you to take up the challenge in this area and continue the excellent start you have already made.

THE VERSATILE COMPUTER: IT MUST BE CONTROLLED

(Institute for Computer Sciences and Technology, National Bureau of Standards, May 1973)

Information Management in a Post-Industrial Society

America's industrial strength was fueled by streams of oil and coal coursing through pipelines and along rail lines into mills and factories. Fuel is still vital, as we know, but the life's blood of today's post-industrial, service-dominated society is information. Erase a few thousand selected computer tapes and essential public services could grind to a halt. Social Security checks would not be written; the contents of warehouses would remain unknown; medical records would be lost.

Of course, no one is going to invade all the tape vaults magnet in hand and bring the country to its knees. But some computer installations have already been wrecked and tapes destroyed in attempts to embarrass government or take vengeance on an employer. (Fig. 1). Happily, these kinds of attacks are on the decline. Computerized fraud, however, is becoming more popular. Bright employees, knowledgeable about the workings of computers and possessing a Robin Hood syndrome, have already stolen millions from banks and corporations. The plain fact is that computers and data banks offer a unique opportunity for sophisticated, intellectual thievery. The TV detective of the future may have to have a degree in computer technology.

Money and goods are not the only objectives of the assaults on computer systems. The acquisition, alteration, or destruction of proprietary or classified information can be of greater consequence than computer-milked savings ac-

counts. Intellectual crimes of the latter type may be either mischievous or malicious in intent.

Far from last is the issue of privacy. A free country cannot tolerate vast data banks filled with personal information on its citizenry unless it has sufficient controls in place to make it feel comfortable. It does not matter whether the data banks are maintained by the government, a credit-rating firm, or an employer; the data therein must be controlled, and, ideally, verified by the affected individual. Theft, alteration, disclosure, and all other forms of misuse must be prohibited by hardware, software and by administrative or electronic controls.

Shutting down the computers is no solution to our problems—we cannot go back to visored clerks pouring over ledgers. Computer systems must be designed with the goal of resolving one of the most vexing problems of our post-industrial society: namely, the Information Paradox epitomized by the demand for:

Freedom of Information;
Privacy of Information; and
Integrity of Information.

These three goals could be mutually incompatible. There can be no privacy if complete freedom of information exchange exists; nor can all personal data be inviolate or the service industries would never know what people want. The proper balance in this triad of goals must be decided by people themselves through the courts and their representatives in government.

The principal targets of the public's concern are: Information, the Computer as the great electronic information machine, and Government as the sole organization with the responsibility and the means to resolve the Information Paradox.

The concern about Freedom of Information culminated in 1966 with the passage of the Freedom of Information Act (Public Law 89–487). This Act amended the "public information" section of the Administrative Procedure Act, and provided for making government-held information available to members of the public unless it comes within specific categories of matters which are exempt from public disclosure. The Act emphasizes that information maintained by the Executive Branch should become more available to the public, while recognizing rights of privacy with respect to personnel and medical records and similar "private" information.

Concern over Privacy of Information manifests itself in a variety of ways. In the Department of Health, Education, and Welfare, then Secretary Richardson in 1970 established an Advisory Committee on Automated Personal Data Systems. The 25-member group is charged with investigating the trend toward data banks containing personal information and the implications of this trend, including invasions of privacy and possible infringement on "due process." The committee has met frequently to hear witnesses testify about the advantages and dangers in the compilation and use of large data banks, the efficacy of the use of the Social Security Number as a universal identification number, and the danger that large files of personal data may be used for other than their original intentions.

There are at least 15 bills before Congress now concerning the issues of privacy and confidentiality of information. Some propose to establish a Federal Privacy Board which would be concerned with questions of the use of personal data files held by the Federal government. Several others are aimed at protecting Federal employees and officials from invasions of privacy possible through the collection of personnel files by their agencies.

Integrity of Information involves the accuracy and timeliness of information in data banks on individuals, their characteristics, and their property. This concern is accentuated by accounts in the popular and technical press about credit-reporting systems and the storage and disposition of arrest records. Individuals have sometimes been denied jobs, housing, or favorable credit ratings on the basis of false, misleading, inaccurate, or out-of-date records.

There is at present no requirement for the operators of data bases to insure the accuracy of their records before disseminating information to requestors. A case in court process now seeks to require that operators inquire on a case-by-case basis into the use of requested information. Any incomplete records, such as an arrest record without a final disposition, should not be disseminated if we are to prevent errors in judgment based on false information. Such information disseminated wrongly could violate an individual's constitutional rights.

The technological, philosophical, ethical, and moral considerations of how information is used and to whom it is disseminated are the crux of the Information Paradox. It has been suggested, for example, that we get out of the habit of

talking about "the computer and privacy"; the problem is "privacy" in itself. Provisions must be established and followed for inspection of records, expunging certain classes of information after specified times, and correcting erroneous and incomplete data.

Wherever the balance point selected by society, the same technology that provides new opportunities for fraud and invasion of privacy also engenders solutions. At NBS we are heavily involved in formulating countermeasures—ways to safeguard the information residing in computers and in transit between them. We call this area of technology "controlled accessibility."

The Magnitude of the Problem

The problem of controlled accessibility is both large in scope and complex. It is big in the sense that there are over 100,000 computers now installed in the United States. It is big in the fact that almost everyone is listed along with certain personal data in one or more data banks. The Mellon Bank of Pittsburg, fourteenth in the nation, processes almost a million checks each day by computer. Travelers Insurance Company assigns 1600 people to data processing and maintains over 130,000 tape reels. The message inherent in such numbers is that there are now an incredible number of machines and people making an even more incredible number of computer transactions and calculations each day. Each person and machine represents a potential avenue of assault on individual privacy proprietary data, and the billions of dollars that flow over communication lines in the guise of computer messages.

Complexity is more difficult to define. Controlled accessibility is at least as complicated as the computer systems themselves; and certainly these are the most sophisticated machines man has designed. No single person completely understands a large computer and even less a network of computers. Thus, no one can really anticipate all attacks that might be made on computer integrity. Not only are computers intellectually unplumbable, they can operate in nanoseconds and rarely leave any "trial" of their activities. One thousand dollars can be transferred to a ficticious bank account in a microsecond unbeknownst to any auditor who might appear on the scene later. These, however, are only technical problems. Figure 2 pictorally depicts the scope and complexity of the computer security problem.

The greatest contributor to the complexity of the situation is the human being. This human being may be inside the computer facility, at a remote terminal, or outside the walls waiting to get in. To some people, the challenge of beating a complex computer system is enticing—like winning at some new kind of electronic chess game. Human ingenuity knows no bounds. Fortunately, this applies to the defense as well as the offense.

Weak Points in Computer Defenses

Nearly every week, newspaper headlines proclaim another big theft by computer-aided criminals. Almost invariably these crimes are inside jobs. (Fig. 3) Some trusted operator, programmer, or maintenance man has used his favorable position to penetrate the computer system through such action as:

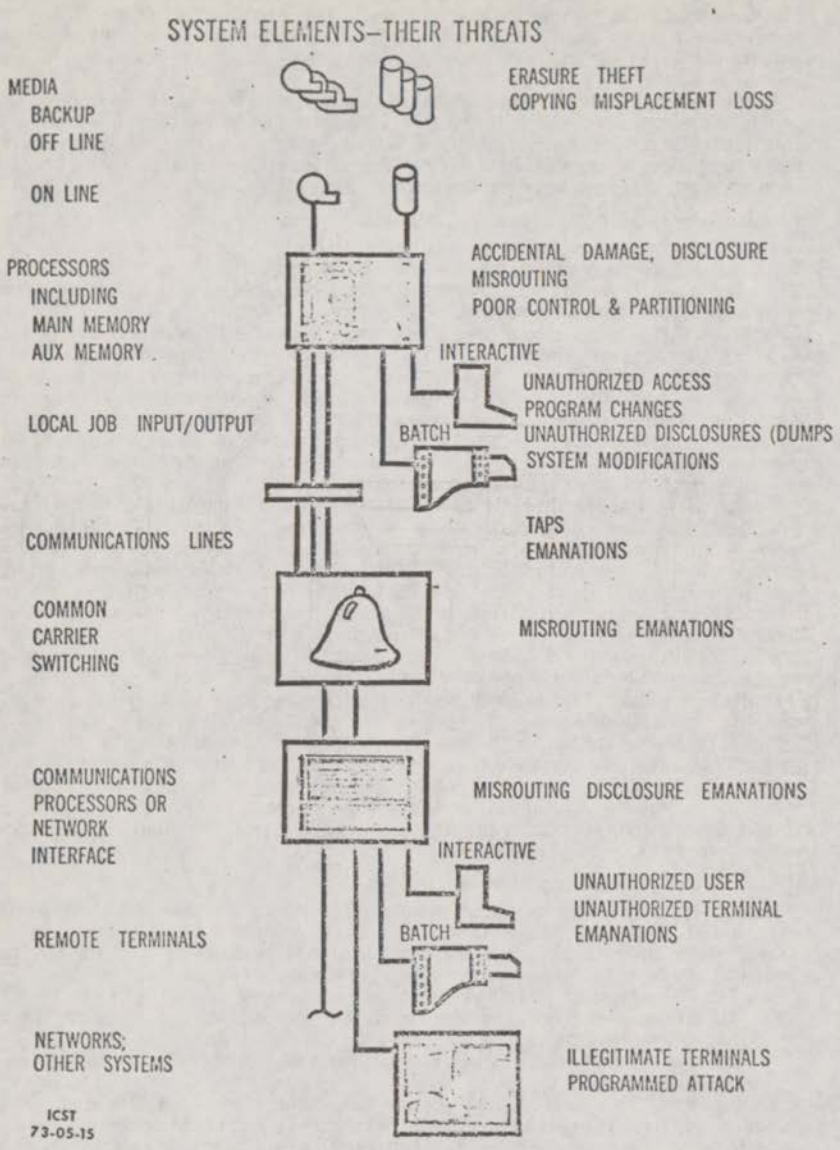
Disabling protective hardware and/or software.

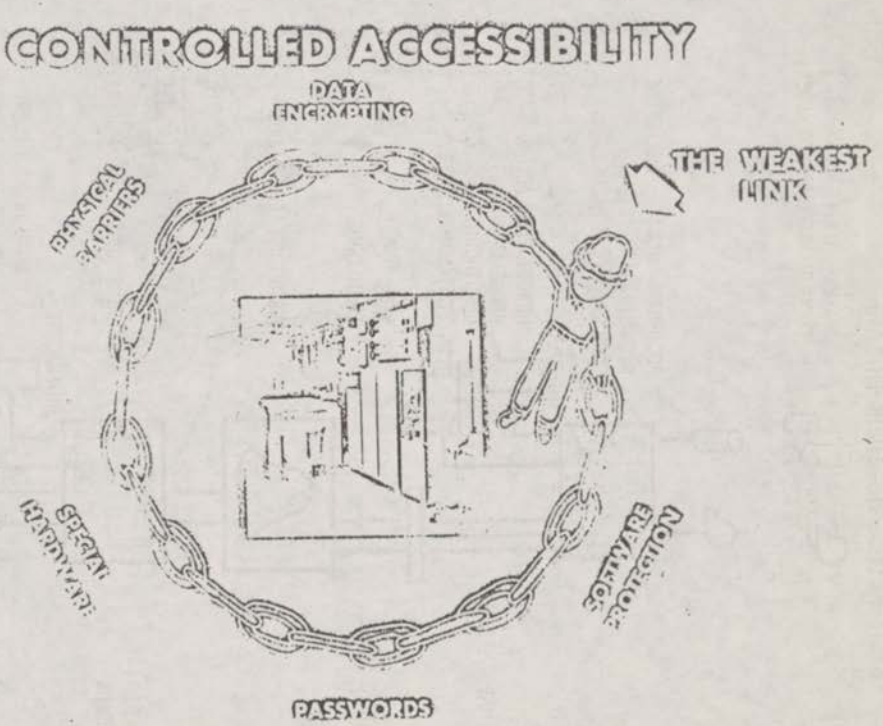
Installing or modifying hardware and/or software to acquire private "ins" or system entries.

Revealing passwords and other protective and entry information to outsiders.

External assaults on computer systems have been rare so far. Perhaps the most dangerous external threat to a computer system is a clever, computerwise individual sitting at some remote terminal. Outside the computer's physical barrier and without fear of surveillance, he can plan and execute sophisticated software probes of the defenses and launch attacks at times of his choosing. In a computer network, one computer can even be used to subvert another. The possibilities are endless and, to some, intellectually challenging.

Computer system defenses can be breached without gaining access to the computer proper or a remote terminal. The weak points for passive subversion are the communication lines and stray electromagnetic radiation leaking from the computer facility. The communication lines can, of course, be bugged intentionally, but sometimes one can hear a great deal in the crosstalk from adjacent communication lines. Microwave links are particularly sensitive to electronic eavesdropping due to the sidelobes of the antenna patterns. Computer facilities are also notoriously leaky insofar as electromagnetic signals are concerned. (Fig. 4) Sensitive instruments can pick up electromagnetic leakage in the air, traveling along electric power lines, and even that induced in the building's plumbing.


SYSTEM ELEMENTS–THEIR THREATS
MEDIA
BACKUP
OFF LINE
ON LINE
ERASURE THEFT
COPYING MISPLACEMENT LOSS
PROCESSORS
INCLUDING
MAIN MEMORY
AUX MEMORY
ACCIDENTAL DAMAGE, DISCLOSURE
MISROUTING
POOR CONTROL & PARTITIONING
INTERACTIVE
BATCH
LOCAL JOB INPUT/OUTPUT
UNAUTHORIZED ACCESS
PROGRAM CHANGES
UNAUTHORIZED DISCLOSURES (DUMPS
SYSTEM MODIFICATIONS
COMMUNICATIONS LINES
TAPS
EMANATIONS
COMMON
CARRIER
SWITCHING
MISROUTING EMANATIONS
COMMUNICATIONS
PROCESSORS OR
NETWORK
INTERFACE
MISROUTING DISCLOSURE EMANATIONS
INTERACTIVE
BATCH
REMOTE TERMINALS
UNAUTHORIZED USER
UNAUTHORIZED TERMINAL
EMANATIONS
NETWORKS;
OTHER SYSTEMS
ILLEGITIMATE TERMINALS
PROGRAMMED ATTACK
ICST
73-05-15



ICST
7.1-05-15

Figure 3.

Active attacks on the integrity of a computer facility resemble conventional cloak-and-dagger activities. Unauthorized persons can gain access through falsified identification badges and bribery. Once inside, a knowledgeable person can do a lot of damage with magnets and the more common tools of sabotage. Passwords can be read from printouts and the defenses cased. If unwatched, the intruder can use the computer itself to erase memories and call up defensive information. Another weak point is the tape vault where files are kept—often under less stringent guard.

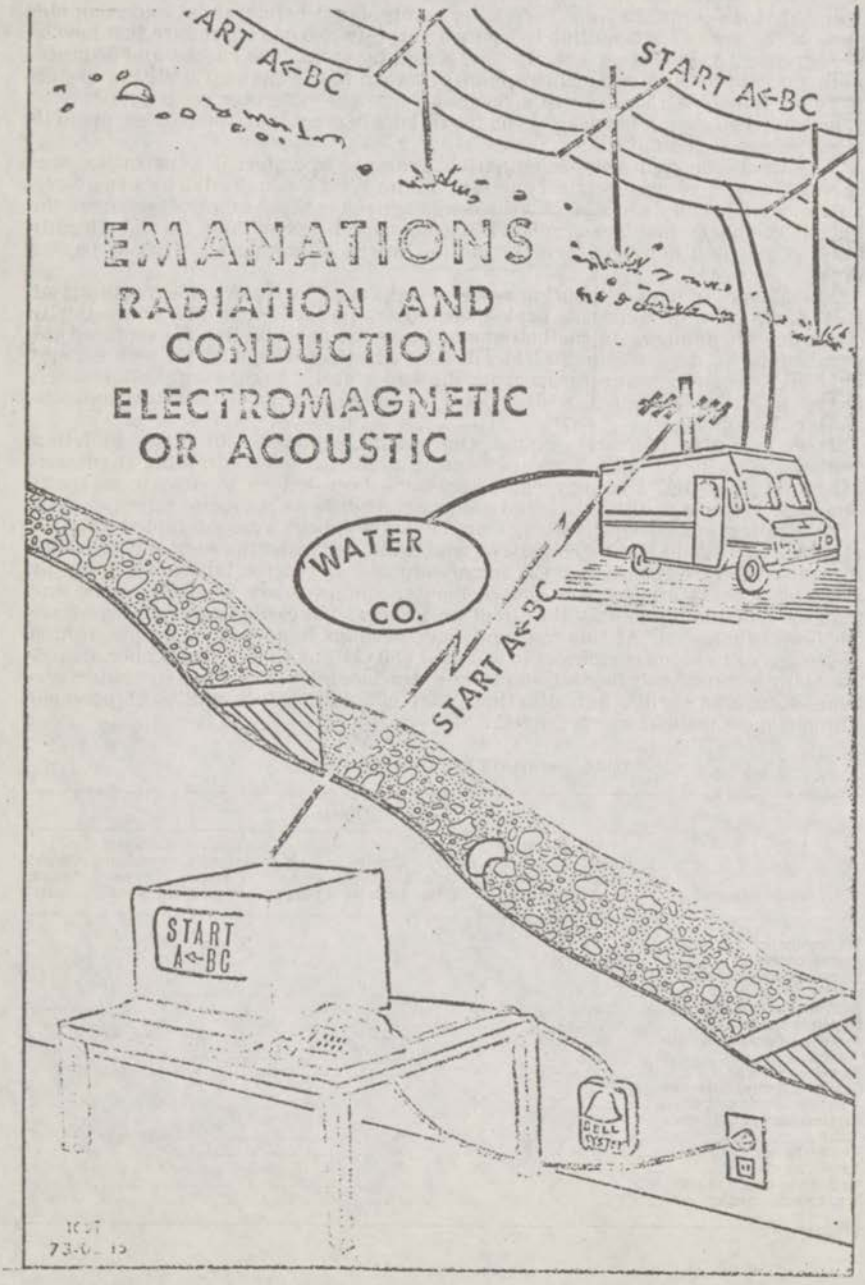


Figure 4.

So far, the emphasis has been on gaining access to the facilities. The computer itself has hardware and software defenses which can be tampered with, circumvented, or which even fail through natural causes. Software defenses include user identification schemes, various access control programs, bounds controls, etc. Software defenses are usually bypassed with software attacks. These attacks can be made more devastating if inside information can be gained first. Once again, the opportunities are limited only by the imagination of the attacker,

Some Typical Assaults on Computer Systems

Computerworld for April 4, 1973, detailed how the Chief Teller of the Union Dime Savings Bank, in New York City, manipulated both manual and computer records to "shuffle" $1.5 million to his own purposes. No one is yet sure just how he accomplished this feat or exactly how much he stole. The checks and balances built into the computer hardware and software and a manual auditing system were all foiled. With access to a terminal—not the computer room proper—the thief switched funds between accounts in such a way that the correct amounts always showed at audit time.

A now classic and very imaginative example of external penetration was carried out by a young electrical engineer on the West Coast. Posing as a customer, he discovered a way to "sign on" the computerized central supply division at the Pacific Telephone and Telegraph Co. Before some betrayed him, he had illegally ordered and had delivered over $1 million worth of equipment without paying for it.

A weak spot in bank computing systems was found by a clerk in a Washington, D.C. bank. Noting that the bank's computer checked only the magnetically coded deposit numbers on the bottoms of incoming deposit slips, he replaced the usual supply of deposit slips on lobby desks with slips coded with his own account number. Depositors using forms from the lobby desks unknowingly added their money to his account. A few days later he made a large withdrawal and disappeared for good.

Other examples of fraud abound. One public employee sold raises to fellow workers. He altered payroll records during nighttime runs, draining thousands out of the treasury. Unhappy employees have been known to commit magnetic sabotage, ruining mailing lists and company records on magnetic tapes.

Two important generalizations can be made about computeraided crimes: (1) most are inside jobs by employees who could not resist the easy opportunities spread out before them; and (2) most were discovered too late and usually by accident. The inferences are that computer defenses are woefully weak and that we very likely see only the tip of an iceberg. The really smart thieves have not been caught yet. At this moment, tens, perhaps hundreds, of people around the country are using computers to criminal ends. Many times this number, including many scrupulously honest employees, are mentally attacking computer systems—vicarious thrills, but situations that could turn into reality if personal circumstances made it worth the risk.

TABLE 1.—THREATS AND COUNTERMEASURES

Countermeasures	Threats							
	Natural catastrophe	Sabotage, hardware and software	Data theft	Copying, browsing, snooping	Bugging	Electromagnetic eavesdropping	Accidental revelation or destruction	Remote terminal assault
Physical barriers	X	X	X	X		X	X	
Guards, badges		X	X	X			X	X
Passwords, fingerprints, voice, signature, etc.			X					X
Encrypting of data			X	X	X	X	X	
EM filters, shields						X	X	
Auditing, checks and balances		X	X				X	X
Threat monitoring		X	X					X
Quality software, data protection, bounds controls		X	X	X			X	X
Personnel screening, motivation		X	X	X				X
Terminal access controls		X	X	X			X	X
File access controls		X	X	X			X	X
Data copies in safe storage	X	X						
Backup support equipment	X	X						

Hardware and Software Defenses

Donn B. Parker, a specialist in computer security at Stanford Research Institute, has said, "The best detective for catching somebody using a computer as a partner in crime is a computer." This statement is equivalent to "Fight fire with fire." This is only part of the answer, however, because additional weapons are needed to defend the computer against its most serious threat: the trusted employee on the inside.

The breadth of the threat spectrum is apparent in Table 1. The countermeasure spectrum is just as extensive; partly hardware, partly software, and partly human judgment and intuition. Computer defenses can be viewed as a series of fortified walls—physical walls outermost, hardware and software on the inside. It is impossible to review all countermeasures here but some generalizations are in order.

First, consider the external threat: an outsider wishing to penetrate the system in order to steal, modify, or destroy data and/or software. The time-honored approach to a good defense is to make the first step toward penetration the biggest; that is, make it exceedingly difficult to become a legitimate user of the computer system. Bricks, mortar, and guards make up the first barrier. (Fig. 5) An interloper who penetrates these barriers confronts next the computer system itself. Will it recognize him for what he is? The computer can check physical attributes: fingerprints, and voice prints, among others. (Fig. 6) It can then ask for a password or other identifying information. Even if the computer allows someone to sign on, he may be stymied by bounds controls, encrypted files, and the sheer complexity of the system. The computer defenses are not completely penetrated until the invader acquires the executive control mode, permitting him to execute any program and read any portion of the memory.

Protective barriers can be made higher and higher against external threats but at a price measured in money and convenience. Furthermore, the most elaborate defenses are largely useless against the insider. It is impossible to place too much emphasis on the careful screening and motivation of employees permitted access to computer facilities.

The most sophisticated defenses can and will be breached by insiders and to a lesser extent by outsiders. Physical evidence of penetration is usually nonexistent, and computer misuse will continue until some lucky accident or human betrayal uncovers the crime. Computer systems should be self-monitoring; that is, they should figuratively ring alarms when suspicious sequences of instructions appear. When a computer is asked to "rewind a printer" or something equally unorthodox, its self-monitoring system should take preventive action. Computers are unsuspicious by nature but software can make them wary. Checks and balances can be built into data processing software to detect bank account shuffling and similar larcenous schemes. Automatic auditing procedures should be used that will provide "audit trails" leading to those probing or subverting the system.

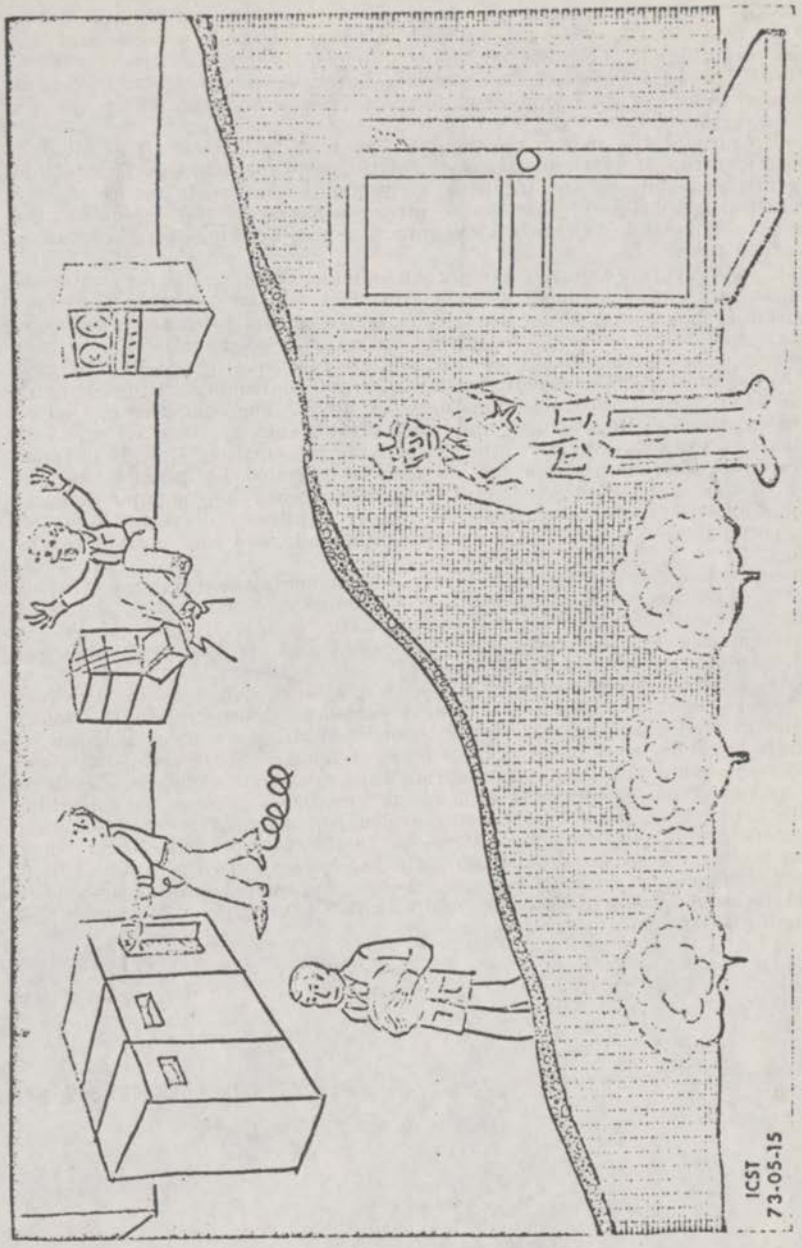


Figure 5. Walls and Guards – Only the first barrier



ICST
73-05-15

Figure 6. A means of personal identificatio

Passive intelligence gathering can pay off surprisingly well with lower risks of detection. One weakness of computer systems lies in the electromagnetic signals they emit. Electrical pulse trains between computer components generate electromagnetic radiation which is transmitted through the air and out along the wires and plumbing pipes penetrating facility walls. Electronic shields and filters are generally adequate to plug such data leaks.

Taps on communication lines connecting computers with remote terminals and other computers necessitate a different approach.

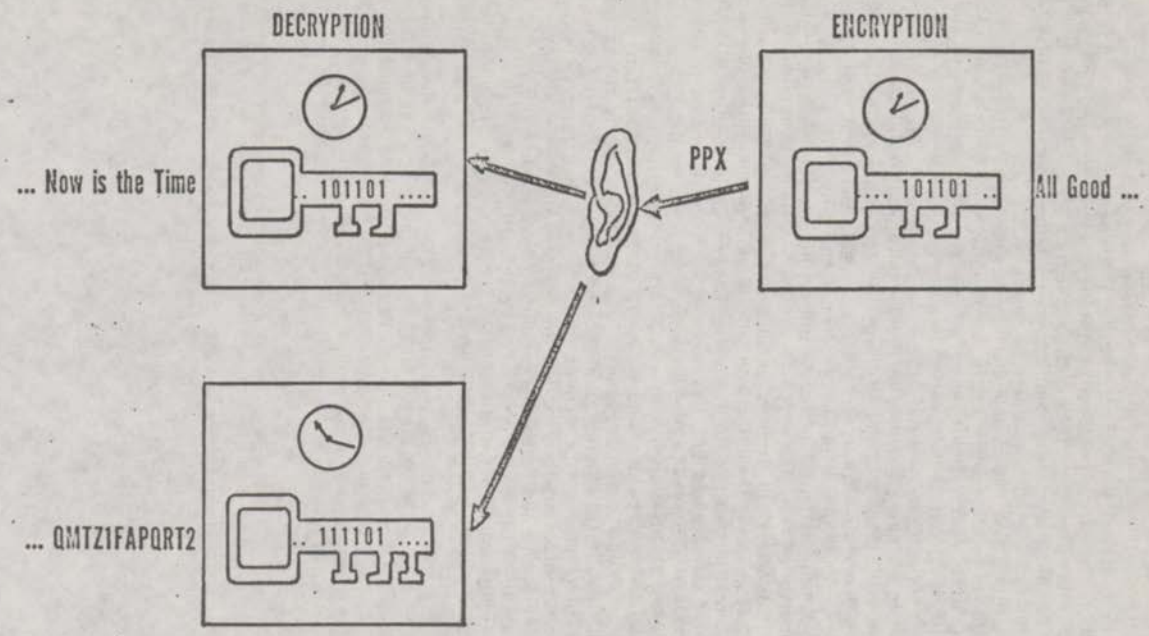
Data encryption (also called enciphering, scrambling, and privacy transformation) is typically an algebraic transformation of a set onto itself. In a computer system, data encryption is generally a transformation of the binary representations of the data onto themselves using an encryption algorithm which has a unique inverse. Performing this inverse algorithm is called decryption.

Encryption algorithms are based on a variable or a set of variables called the encryption key. (Fig. 7) This key must be distributed to all points where encryption and decryption are to occur using a specialized, protected distribution system. Thus, the data protection is based on both an algorithm and a protected key. Usually, the algorithm is generally known but the key is highly protected and often changed.

Encryption protects data during transmission between a computer and its terminals and other computers. Data in storage is often encrypted, as are passwords. An interesting feature of protecting passwords is that they can be encrypted with an algorithm which has no inverse. A user-supplied password can simply be encrypted and used in that form, making it impossible for an operator, maintenance man, or programmer to obtain all information in the system.

Layers of defensive hardware and software consume more machine time and make computer systems less convenient to use. The more secure the system, the more it costs to use. In this context, it should be noted that, despite the headlines about million-dollar thefts, the amount of computer-aided theft is still rather small. By far the biggest source of loss in business data processing operations originates in the errors and omissions committed by honest employees. The software audits and tests for consistency being designed to catch criminals will also help eliminate innocent errors and omissions. In fact, the savings accrued here may well pay for all the paraphenalia needed to control access and insure data security.

CRYPTOGRAPHY: A PARTIAL SOLUTION



ICST
73-05-15

Figure 7.

The NBS Role in Controlled Accessibility

Many organizations within government and in the private sector are working on computer security. The Department of Defense, for example, has issued directives in the areas of emanations and data processing security requirements.[1] The Government Management Information Systems (G–MIS) Organization has written a first-draft manual on administrative guidelines for government data centers.[2]

Many private companies are funded by the government to carry out research and development in voice recognition, operating system redesign, and the like.

In addition, individual companies recognizing the importance of the problem are concentrating their own resources in this area. To illustrate, IBM has initiated the following four programs:

1. TRW Systems: Certification and measurement techniques.
2. State of Illinois: Evaluation of the impact of security procedures on operations.
3. MIT: Authorization technology.
4. IBM—Gaithersburg: Project control and system implementation.

The implementing mechanisms listed below are primarily applicable to Federal agencies but will also be useful to state and local governments. In addition, through cooperative efforts now underway by government with professional societies and trade associations, they should also have significant utility in the private sector.

1. Legal requirements and directives
2. Standards and guidelines
3. Specifications
4. Measurement techniques
5. Certification or evaluation procedures
6. Regulations

Within the wide scope of activities supporting these policy mechanisms, the NBS is concentrating its resources on a small but important subset. The National Bureau of Standards has only a very minor role, of course, in the development of regulations, legal requirements and directives, but it has an important part to play in the development and implementation of the other four mechanisms listed (2 through 5).

In particular, the NBS effort concentrates on the standards and guidelines that will allow for the control of accessibility to computer systems and for specification of levels of assurance of security. These are probably among the most important means available for meeting the demands being established by Congress, the Executive Branch, consumer groups, and legal organizations. Controlled accessibility measures provide an essential means for countering the threats identified on Table 1.

---

[1] DOD Directive 5200.19. Control of Compromising Emanation. February 10, 1968.
DOD Directive 5200.28. Security Requirements for Automatic Data Processing (ADP Systems.) December 18, 1972.

[2] (72.01 draft) An Administrative Guideline for Security and Confidentiality in State and Local Government Data Centers, November 17, 1972.

TABLE 2.—WORK ON IMPLEMENTING MECHANISMS AIMED AT SOLVING THE PROBLEM OF CONTROLLED ACCESSIBILITY

Implementing mechanism	Components of task										
	Data sensitivity	Processing environment	Man-system interface	User identification	Access devices	Access control features	Physical access, personnel, etc.	Performance evaluation	Security levels	Communication	Encryption
Legal requirements and directives	X Congress						X		X		
Standards and guidelines		NBS*	NBS*				X	NBS	NBS*		NBS
Specifications				NBS		NBS*		X	NBS		NBS
Measurements techniques				X		NBS*	NBS	NBS	NBS		NBS
Certification and evaluation					NBS* NSA	X			X		
Regulations					X	X			X	FCC	

* Indicates highest NBS priority; NBS=NBS active project; DOD=DOD active project, etc.; X=work needed.

In order to allocate scarce resources effectively within NBS and the Federal Government, the controlled accessibility problem has been broken down into components which can be addressed simultaneously by technical groups inside and outside the Federal Government. These components are listed along with applicable implementing mechanisms in Table 2. The areas where NBS is concentrating its resources are delineated. Asterisks signify highest priority. When an area is given top priority by NBS, it means that NBS is recommending to OMB as well as the Department of Commerce that all agencies should focus their attention here; not that NBS should be or can be the sole or principal organization involved.

Specific NBS/ICST Efforts

NBS will concentrate its own resources (and recommend the same for the Federal Government as a whole) on providing a rapid technical solution to the controlled accessibility problem. The solution must include means for positive identification of remote users, adequate communications security, and tamper-proof access control mechanisms. The identification problem already addressed by ARPA and other mission-oriented agencies will be a major portion of the ICST FY 1975 programs. Here, Federal guidelines and standards will be generated where possible.

In FY 74, specific guidelines will be developed and published which will help managers of Federal computer installations evaluate their risks and determine what actions should be taken to minimize their risks in a cost-effective manner. Guidelines for the development of encryption algorithms and the design of secure operating systems will follow in FY 75.

The study of the effects of magnetic fields on stored data (NBS Tech Note 735) will be continued. This area has attracted the attention of the popular and "underground" press and is the subject of much misunderstanding. The NBS Tech Note aims at reducing that misunderstanding.

Quantitative measures for risk and effectiveness will be developed. The risk measure will include both the processing environment and the sensitivity of the data being processed. The fundamental principles of measuring the level of computer security will be identified.

Criteria will be developed for processes and procedures included in the design of secure operating systems. These will provide managers and system designers with tools for evaluating present systems, for writing procurement specifications, and designing secure operating systems. The design cycle of computer systems is a long one, and it is crucial that work on these tasks begin as soon as possible.

Table 3 summarizes planned products with an accompanying schedule for their delivery.

Validation techniques will be developed for access control mechanisms. Current testing techniques consist of trial and error attempts to defeat the access control features. The results of such a test are conclusive only in a negative sense. It can be shown that a system can be broken, but not, at the present time, that a system cannot be broken.

The problem of positive identification requires the exploration of the technologies of fingerprint identification, voiceprint identification, and others to develop a cost-effective means of identification. The use of encryption of data on storage media and evaluate commercial security devices relative to Federal needs will also be investigated.

A cooperative venture between NBS and the Association for Computing Machinery was begun last year. In December 1972, a joint NBS/ACM workshop was held on controlled accessibility. Experts in the field of computer security met and grappled with the problems of access control mechanisms, audit techniques, management control, identification, and measures. An attempt was made to interpret research results as well as determine those areas where significant questions remain unanswered. Several publications will result from this workshop. Another joint workshop on the subject of privacy was held in February 1973.

TABLE 3.—NBS/ICST GOALS IN THE AREA OF CONTROLLED ACCESSIBILITY

Anticipated goals and results	*Dates available*
Guidelines for achieving physical security	1st quarter, fiscal year 1975.
Guidelines for developing encryption algorithms for data transmission	2d quarter, fiscal year 1975.
Guidelines for designing secure operating systems	Do.
Quantitative measures for determining risks and effectiveness of security techniques [1]	3d quarter, fiscal year 1975.
Techniques for evaluating security devices for positive identification of individuals [1]	4th quarter, fiscal year 1975.
Fundamental principles of computer security measurement techniques [1]	Do.
Techniques for validating access control mechanisms [1]	3d quarter, fiscal year 1976.

[1] Dependence upon fiscal year 1975 budget increase.

On a continuing basis, NBS is collecting information on both the legal and technical aspects of computer security. This repository of information permits the answering of inquiries and in general is an important source of information on controlled accessibility for the non-defense Federal establishment.

NBS is intensifying efforts to develop and implement those mechanisms which will enable both government and industry to achieve high utilization of their computer systems while at the same time meeting their responsibilities for privacy and security in a cost-effective manner.

STUDENT RECORDS

[From the Congressional Record, Senate, May 9, 1974]

PROTECTION OF THE RIGHTS AND PRIVACY OF PARENTS AND STUDENTS

Mr. BUCKLEY. Mr. President, in the last few years a considerable amount of effort has been expended to investigate and expose the dangers and injustices created by the secret compilation and dissemination of data and files on the personal lives and business affairs of millions of Americans, who have had no opportunity to review the material in these files and to correct the many errors and hearsay that are often found therein.

We are all familiar with stories of both serious outrages and humorous foulups caused by erroneous material stored in various data banks or credit department computers. Trivial or erroneous material kept in such files can harm and haunt individuals throughout their lives.

The public has also become aware of the genuine danger to the privacy and civil liberties of all Americans posed by the growth of such secret files and computer banks. Several bills have been introduced in Congress to attempt to deal with this problem, and I am pleased to be a cosponsor of one of the most significant ones, S. 2883, the Fair Credit Reporting Act of 1974.

But, Mr. President, in spite of this evidence of increased awareness and concern over these dangers, hardly any public outcry has been heard about the systematic violation of privacy and personal rights, through the existence of secret files, of two of the largest classes of Americans.

I speak of the right of privacy of millions of children in the schools across our Nation whose school records are routinely made available to governmental and other busybodies, and the rights of their parents, who are too often denied access to such information.

The serious problems and dangers posed by secret files in our schools were well described in a recent article by Diane Divoky in Parade magazine entitled, "How Secret School Records Can Hurt Your Child." I ask unanimous consent that the article be printed at the end of my remarks.

Miss Divoky notes that—

"Recent surveys of representative school systems throughout the country found that CIA and FBI agents and juvenile court and health department officials had access to the entire records in more than half the schools systems: local police in 33 percent and parents in less than 10 percent."

These records contain not only test scores and medical reports, but also many so-called anecdotal comments which can haunt a child throughout his school years and beyond. A staff member of the New York Civil Liberties Union has stated that—

"There is tremendous abuse in the preparation of these records. Teachers will think nothing of inserting comments like, 'I feel sorry for the teacher who gets this kid next year,' of 'This one is really a gem.' "

As a result, children may become permanent victims of their teachers' prejudices or misconceptions.

But the issue of secret school records is only a part of a larger problem of the violation of privacy and other rights of children and their parents that increasingly pervades our schools.

Many schools do not ask parents' permission to give personality or psychiatric tests to their children, or to obtain data from the children on their parents and family life. Some of these tests include questions dealing with the most personal feelings and habits of children and their families. Some of these data, in personally identifiable form, is given to other government agencies or to private organizations. Some of it ends up on Federal computers in the caverns of the Department of Health, Education, and Welfare. Just this past March a Federal

office demanded personally identifiable educational, ethnic, and family information on over 100,000 New York City's elementary school pupils. Fortunately, the city board of education adamantly refused, even in the face of a reported threat to cut off all Federal education funds—over $200 million a year—to the city.

Attempts are, of course, made to excuse the collection and dissemination of such "data," which is in most cases not accessible for review by parents or students, on the basis that this is all done "in the best interest of the student." In my own State, the Parent-Teachers Association has rejected such assertions, and has taken a strong stand against these abuses, and has called for their correction.

But there have been additional abuses of the rights of children and their parents. In some instances children are required to participate in experimental education programs, in medical research, or in programs or activities designed to affect their personal behavior, values, or social development—without their parents' adequate knowledge or consent. The Children's Defense Fund, headquartered here in Washington, has documented many disturbing cases of such abuses across the country.

Often the instructional materials in experimental and other school programs and courses are not readily available to parents for inspection and review. In those cases where parents have been able to obtain copies of restricted materials, they have frequently found them to contain items and ideas that are not only controversial, but also in direct opposition to the moral values and beliefs of many parents.

Such secrecy, such denials of the right of parents to find out what is being taught and one to their children in school, reflect an elitist arrogance on the part of many in the educational establishment which is shocking.

Some educators seem to have forgotten that parents have the primary legal and moral responsibility for the upbringing of their children and only entrust them to the schools for basic educational purposes. This entrusting to the schools is not an abdication of parental rights and responsibilities, but rather a sharing of them by the parents.

Yet, some educators seem to feel that they know much more about the welfare and best interests of the child than do the parents, and therefore, once a child comes under their sway, they think they have the right to do what they themselves think is best for the child, without regard for values and beliefs of the parents.

Mr. President, it is time we take the lid off secrecy in our schools. We have passed a Freedom of Information Act to remove much of the secrecy involved in the activities of the Federal bureaucracy and to make information available to the public which should rightly be theirs. It is high time that we pass a Freedom of Information Act for children and parents.

Therefore, Mr. President, I propose an amendment to S. 1539, which will add a new section to the bill, entitled, "Protection of the Rights and Privacy of Parents and Students." I send it to the desk and ask that it be printed. I also ask unanimous consent that the amendment be inserted in the Record at the end of my remarks.

I am happy to say that in offering this amendment I am joined by the distinguished senior Senator from North Carolina, Senator Ervin, as well as Senator Curtis, Senator Goldwater, Senator Tower, Senator Dole, Senator Brock, Senator McClure, Senator Gurney, Senator Helms, Senator Thurmond, and Senator Biden.

I want to add that after I first circulated this amendment last week, I received several suggestions and helpful criticisms from other Senators and some interested organizations, such as the National School Boards Association and the Children's Defense Fund of the Washington research project, about certain problematic portions or omissions in the amendment. I have taken these suggestions into consideration, and have made several modifications in some of the language which I think should satisfy many of the basic concerns which were raised.

Some may ask: "Why talk about problems and abuses of local school administration? Why should this be a concern of Federal legislation to aid education?"

First, let me note that programs of Federal aid to the States and localities have almost always required that the recipients meet certain conditions—the area of civil rights and nondiscrimination being one of the most prominent examples—in order to be eligible for assistance. My amendment serves to make the protection of civil rights more comprehensive.

Second, the fact is that in many cases, the collection and dissemination of various personal data and the development of various experimental and attitude-affecting programs have been not only encouraged and sponsored, but often mandated as a condition for assistance by HEW and the Federal Office of Education, acting under the broad and vague authority granted them by Congress. The aforementioned affair in New York City is a case in point, as is a recent case in Howard County, Md., where an NIE grant to Johns Hopkins University resulted in testing there in the public schools for extensive personal and family information, without parental knowledge or consent. And just this week the Washington papers reported that the District of Columbia school board has refused to administer a test to its students which the Federal Office of Education has demanded that it give.

Thus, the Federal Government is directly involved in perpetrating and perpetuating many of the abuses of which I have spoken. My amendment specifically relates to school programs, projects, and activities which are sponsored or assisted by the Federal Government under the various education laws being amended by S. 1539.

My amendment will help to provide parents with access to their children's school records, to prevent the abuse and improper disclosure of such records and data, and to restore the rights of privacy to both students and their parents.

In addition, it will reinforce the rights and responsibilities of parents with respect to the education of their children by requiring parents' permission before their children are made to undergo certain forms of testing or partake in certain experimental or attitude-affecting programs or activities, and by requiring that instructional materials used in school be available to parents, upon reasonable request, for their inspection and review.

In addition, my amendment requires the Secretary of Health, Education and Welfare to adopt appropriate safeguards to protect the rights of privacy of students and their families in regard to Government-authorized surveys and other data gathering activities.

In the wake of recent scandals over Government spying and secrecy, President Nixon announced the establishment of a high-level committee to provide a "personal shield for every American" against all invasions of privacy. Surely we must not exclude our children from this protection. Mr. President, the Senate can act now to affirm the privacy and rights of children and their parents by adopting my amendment.

Mr. President, I ask unanimous consent that excerpts of an interview with Marian Edelman, director of the Children's Defense Fund of the Washington Research Project, be inserted at this point in the Record, as well as sample "parental consent" forms prepared by the Russell Sage Foundation.

There being no objection, the amendment and material were ordered to be printed in the Record, as follows:

Calendar No. 735

93D CONGRESS
2D SESSION

S. 1539

IN THE SENATE OF THE UNITED STATES

MAY 9, 1974
Ordered to lie on the table and to be printed

AMENDMENTS

Intended to be proposed by Mr. BUCKLEY (for himself, Mr. BIDEN, Mr. ERVIN, Mr. BROCK, Mr. CURTIS, Mr. GOLDWATER, Mr. TOWER, Mr. MCCLURE, Mr. DOLE, Mr. GURNEY, Mr. HELMS, Mr. THURMOND to S. 1539, a bill to amend and extend certain Acts relating to elementary and secondary education programs, and for other purposes, viz:

On page 330, between lines 17 and 18, insert the following new section:

"PROTECTION OF THE RIGHTS AND PRIVACY OF PARENTS AND STUDENTS

"SEC. 437. (a) RIGHT OF ACCESS AND OF A HEARING.—(1) No funds shall be made available under any applicable program to any State or local educational agency, any institution of higher education, any community college, any school, preschool, or any other educational institution

which has a policy of denying, or which effectively prevents the parents of students under eighteen years of age attending any school of such agency, or attending such institution of higher education, community college, school, preschool, or other educational institution, the right to inspect and review any and all official records, files, and data directly related to their children, including all material that is incorporated into each student's cumulative record folder, and intended for school use or to be available to parties outside the school or school system, and specifically including, but not necessarily limited to, identifying data, academic work completed, level of achievement (grades, standardized achievement test scores), attendance data, scores on standardized intelligence, aptitude, and psychological tests, interest inventory results, health data, family background information, teacher or counselor ratings and observations, and verified reports of serious or recurrent behavior patterns. Where such records or data include information on more than one student, the parents of any student shall be entitled to receive, or be informed of, that part of such record or data as pertains to their child. Each recipient shall establish appropriate procedures for the granting of a request by parents for access to their child's school records within a reasonable period of time, but in no case more than forty-five days after the request has been made.

"(2) Parents shall have an opportunity for a hearing to challenge the content of their child's school records, to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading, or otherwise inappropriate data contained therein.

"(b) PARENTAL CONSENT.—(1) No student shall, as a part of an applicable program, be required to undergo medical, psychological, or psychiatric examination, testing, or treatment, or immunization (except to the extent necessary to protect the public from epidemics of contagious diseases), or to reveal information about his or her personal or family life without the prior, informed, written consent of the student's parents.

"(2) No student shall, as a part of any applicable program, be required, without the prior, informed, written consent of the student's parents, to participate in any project program, or course, the primary purpose or principle effect of which is to affect or alter the personal behavior or personal values of a student, or to explore and develop teaching techniques or courses primarily intended to affect such behavior and values.

"(3) Parents shall be informed, reasonably in advance and in writing, of the intended participation of their child

in any research or experimentation project which is a part of an applicable program. No child shall participate in such a project if the parents of such child object to such participation.

"(4) As used in this subsection the term 'research or experimentation project' means any project or program which is a part of an applicable program, and which is authorized by an administrative officer of an education agency, a State or local education agency, or any education institution, including preschools, for the purposes of research or experimentation, except that research or experimentation projects shall not include projects in the field of reading or bilingual education, as determined by the Commissioner.

"(c) CONDITIONS FOR THE RELEASE OF PERSONAL DATA.—(1) No funds shall be made available under any applicable program to any State or local education agency, any institution of higher education, any community college, any school, preschool, or any other educational institution which has a policy of permitting the release of records or files (or personal information contained therein) of students without the written consent of their parents to any individual, agency, or organization, other than the following—

"(A) other school officials, including teachers within the educational institution or local educational agency who have legitimate educational interests;

"(B) to officials of other schools or school systems in which the student intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record.

"(2) No funds shall be made available under any applicable program to any State or local educational agency, any institution of higher education, any community college, any school, preschool, or any other education institution which has a policy or practice of furnishing, in any form, any information contained in personal school records, to any persons other than those listed in subsection (c) (1) unless—

"(A) there is written consent from the student's parents specifying records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents, or

"(B) such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpena, upon condition that parents and the students are notified of all such orders or subpenas in advance of the compliance therewith by the education institution or agency.

"(3) In any case in which the Secretary or an administrative head of an education agency is authorized under any applicable program to request or require any State or local educational agency, any institution of higher education, any community college, any school, preschool, or any other educational institution to submit to a third party (or to the Secretary or an administrative head of an education agency, as defined in section 409 of this Act) any data from personal statistics or records of students, such data shall not include the names of students or their parents (in code or otherwise) without the written consent of the student's parents, except—

"(A) in connection with a student's application for financial aid;

"(B) in compliance with any court order, or pursuant to any lawfully issued subpena, if the parents and students are notified of any such order in advance of the compliance therewith by the State or local educational agency, the institution of higher education, the community college, the school, preschool, or other educational institution.

"(4) (A) With respect to subsections (c) (1) and (c) (2) and (c) (3), all persons, agencies, or organizations desiring access to the records of a student shall be required to sign a written form which shall be kept permanently with the file of the student, but only for inspection by the parents

or student, indicating specifically the legitimate educational or other interest that each person, agency, or organization has in seeking this information. Such form shall be available to parents and to the school official responsible for record maintenance as a means of auditing the operation of the system.

"(4) (B) With respect to this subsection, personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.

"(d) PROTECTION OF PERSONAL DATA.—The Secretary shall adopt appropriate regulations to protect the rights of privacy of students and their families in connection with any surveys or data-gathering activities conducted, assisted, or authorized by the Secretary or an administrative head of an education agency (as defined in section 409 of this Act). Regulations established under this subsection shall include provisions controlling the use, dissemination, and protection of such data. No survey or data-gathering activities shall be conducted by the Secretary, or an administrative head of an education agency have responsibilities under an applicable program unless such activities are authorized by the Act establishing such a program.

"(e) For the purposes of this section, whenever a stu-

dent has attained eighteen years of age, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student.

"(f) No funds shall be made available under any applicable program unless the recipient of such funds informs the parents of students, or the students, if they are eighteen years of age or older, of the rights accorded them by this section.

"(g) The Secretary, or an administrative head of an education agency, shall take appropriate actions to enforce provisions of this section and to deal with violations of this section, according to the provisions of this Act.

"(h) The Secretary shall establish or designate an office and review board within the Department of Health, Education, and Welfare for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions of this section and complaints which may be filed concerning alleged violations of this section, according to the procedures contained in subsections (c) and (d) of section 421 of this Act.

"(i) With respect to any funds obligated prior to the effective date of this section to any State or local educational agency, any institution of higher education, any community college, any school, preschool, or any other educa-

37-583 O - 74 - pt. 2 - 54

tional institution, continued furnishing of such funds shall cease January 1, 1975, if the recipient has failed to meet the conditions for funding established by this section.

"(j) The provisions of this section shall become effective ninety days after the date of enactment of this Act.

"(k) This section may be cited as the 'Family Educational Rights and Privacy Act of 1974'."

On page 122, in the table of contents, after the item "Sec. 512" insert the following:

"Sec. 513. Protection of the rights and privacy of parents and students.".

[From the Parade magazine, Mar. 31, 1974]

How Secret School Records Can Hurt Your Child

(By Diane Divoky)

"An habitual liar and a real sickie." "Ego-impaired and maladaptive." "Unnaturally interested in girls." "A real show-off in class, probably because of serious problems at home."

Who are these problem students? They're your children and mine, as described in increasingly fat folders maintained by the schools.

Student records—any teacher or school counselor will tell you—are used more and more to get a picture of the "whole child," his family, and his psychological, social and academic development. So besides hard data, such as IQ scores, medical records, and grades, schools are now collecting files of soft data: teachers, anecdotes, personality rating profile, reports on interviews with parents, and "high security" psychological, disciplinary and delinquency reports. These are routinely filed away in school offices or stored in computer data banks.

You, the parent, probably can't see most of these records, or control what goes into them, much less challenge any untrue or embarrassing information they might contain. But a lot of other people—the school office clerk, potential employers, probation officers, welfare and health department workers, Selective Service board representatives, and just about any policeman who walks into the school and flashes a badge—have carte blanche to these dossiers on your child. And to top it all off, parents are never told who's been spying on their children.

OTHERS HAVE ACCESS

Recent surveys of representative school systems throughout the country found that CIA and FBI agents and juvenile court and health department officials had access to the entire records in more than half the school systems; local police in 33 percent and parcels in less than 10 percent.

Even in the rare states or districts where parents have a legal right to inspect records, that right is often denied in practice. As a principal in a California suburb put it: I know what the law is here in California. Parents are supposed to be able to see the cumulative record. But if a parent comes in and asks to see a record, first I ask why. If there's a really good reason, I'll share some of it with them—but there are certain items I'll always withhold."

OFFICIAL ARROGANCE

The schools argue that student records are their records, to share with whom they choose "for the benefit of the child." Forgetting that parents have the basic legal and moral responsibility for their child and only entrust the child to the school for educational purposes, many school officials arrogantly assume that somehow they know more about the welfare of the child.

A third of the schools do not ask parents for permission before collecting personality test data, and half don't get parents' permission before collecting data on families. Sixteen percent of the systems don't get any form of parental consent before submitting students to psychiatric tests. School counselors, who keep some of the most sensitive records, insist that they'll have to water down their records if they know parents may see them, an argument that raises provocative questions about what goes into those records, and about the school's attitudes toward parents. The results of the school's attitudes, in practice:

A community tutoring projects' secretary calls an elementary school to check on a student's grade placement, and the principal gratuitously reads from the record that the child is a bed-wetter, and that his mother is an alcoholic with a different boyfriend in the house each night.

A mother sneaks a look at her junior high school son's record, and sees that back in second grade an anonymous teacher had written: "exhibitionist tendencies." After several months of work running down the teacher, who no longer taught in the school system, she discovered that the comment was based on a single incident when the youngster had hurriedly returned from the lavatory unzippered.

A black father who works for the school his daughter attends gets to see her file, and finds five pages of notes about his and his wife's "political activity."

A parent is informed by a guidance counselor, about to write a college recommendation for her son, that his "psychological" file labeled him a "possible schizophrenic" back in elementary school. The mother didn't know such a file existed.

The parents of a junior high student are told their daughter won't be able to attend graduation ceremonies because she's a "bad citizen." What has she done that's bad, the parents ask. Well, the principal says, the school had a whole file on her "poor citizenship," but the parents can't know what's in that file. In this Catch-22 case, one of the few to get a legal hearing, the New York State Commissioner of Education, Ewald B. Nyquist, stated flatly that the school's argument—that it was acting in the best interest of the student in refusing to reveal the information to the parents—had "no merit." The commissioner concluded: "It is readily apparent that no one had a greater right to such information than the parents."

TREMENDOUS ABUSE

"Most people don't even know their rights on this issue," says a staff member of the New York Civic Liberties Union.

"There is tremendous abuse in the preparation of these records. Teachers will think nothing of inserting comments like, "I feel sorry for the teacher who gets this kid next year,' or "This one is really a gem.' "

A 9-year-old boy who once hugged a classmate had "homosexual tendencies" written into his permanent record.

Even an affectionate, harmless kiss on the cheek can be interpreted by an overzealous teacher as an "unnatural interest in girls."

In one case, the parents of a 7-year-old boy who was killed accidentally obtained his school records in the litigation that ensued. Some of the comments they found: "Can read and do numbers, but is too immature"—this at the end of the first grade; and "Refuses to use left hand—dislikes being reminded to try." Not mentioned was the fact that the boy had an orthopedic problem on his left hand.

A high school student who criticized his principal on a radio station had "radical tendencies" placed in his record.

"It's an insidious problem," says the NYCLU official, "because most people don't even know who has seen their records and if they are being discriminated against as a result."

Concerned about the growing potential for abuses in school record keeping, the Russell Sage Foundation published in 1969 a widely distributed set of guidelines to aid school systems in establishing fair policies and practices. But five years later, the vast majority of school systems haven't gotten the message. The New York City Board of Education finally established good policies, but few parents or students there seem to know about the protections.

PROTECTIVE LEGISLATION

Des Moines, Iowa, and Jefferson City, Mo., have taken steps to safeguard records, and at the state level, Oregon and New Mexico have passed legislation to give parents and older students access to records, and to protect records from outsiders. New Hampshire bans records that tell of students' political beliefs and activities, and Delaware gives students control of their own records once they are 14 years of age. Elsewhere, the easy flow of information and misinformation—from school to police to social agency—goes unchecked.

One group that is concerned about the problem, the National Committee for Citizens in Education, headquartered in Columbia, Md., urges parents to take a stand—to find out if you can see all of your children's school records, and what provisions your school has to protect records from outsiders' eyes. The committee is preparing a state-by-state guide of school record laws to tell parents where they stand, plus a handbook to guide parents and citizens in asking the questions that will give you the answers on school records policies and practices in your district. It will also provide you with model codes that your state board of education or school system might adopt.

If all else fails, the committee will even tell you how to proceed with legal action. You can write to the National Committee for Citizens in Education, Suite 410, Wilde Lake Village Green, Columbia, Md. 21044.

Last month President Nixon announced that he was setting up a top priority committee headed by Vice President Ford to provide a "personal shield for every American" against invasions of privacy from any source; surely this must apply to our children, too.

[Sample form A]

ROUTINE INFORMATION LETTER TO BE SENT HOME AT BEGINNING OF EACH SCHOOL YEAR OR AT TIME STUDENT ENROLLS DURING YEAR

Dear Parent, In accordance with the recommendations of the Superintendent of Schools and the Director of Measurement and Evaluation, the Board of Education has approved a city-wide testing program designed to provide information concerning the proficiency of all children in the district on standardized tests of academic achievement and aptitude.

The result of these tests provide a continuing record of each child's academic progress in comparison with national norms. They are also an invaluable aid to your chlid's teacher and counselor in diagnosing individual strengths and weaknesses in order to provide more effective individualized instruction. During the coming school year the following tests will be administred to your child as part of this program:

(Example)

Name of test: Iowa Tests of Educational Development, Grade 10.
Purpose: Measurement of achievement in mathematics, English, basic science.
Name of test: Terman-McNemar Test of Mental Ability.
Purpose: Measurement of verbal and mathematical aptitude.

Your child's scores on these tests will be checked carefully and maintained in the school record as long as your child attends school in this system. Should your child transfer to another school system, you will be notified of the transfer of his or her permanent record to the new school system. No individual or agency outside of the school system will be permitted to inspect your child's school record without your written permission.

Should you wish to examine your child's record file at any time you may arrange to do so by making an appointment with the principal's office. [In addition, a routine report and interpretation of your child's scores on the abovementioned tests will be included as part of the second term grade report.]

Sincerely,

_____,
Superintendent of Schools.

[Sample form B]

REQUEST FOR PERMISSION TO COLLECT PERSONAL DATA

SPECIAL REQUEST FOR PERMISSION TO COLLECT PERSONAL INFORMATION

In order to provide your child with more effective guidance and counseling services, your permission is requested for the collection of the following kinds of personal information from your child.

(Example)

Type of Information or Test:
Minnesota Multiphasic Personality Inventory.
Kuder Preferenec Record.
Wrenn Study Inventory.
Family Background Information.
(NOTE.—Space provided for description and purpose: permission granted; permission denied.)

Because of the sensitive nature of this informtion, all test scores and related information will be treated with complete confidentiality. Only parents and authorized school personnel will be permitted access to this information without parental consent.

Please check the appropriate box signifying your approval or disapproval of this request, sign the form in the space provided below, and return in the enclosed envelope.

[Sample form C]

RECORD OF INSPECTION OF PUPIL RECORDS

Date —.
Records examined —. (Name of pupil or pupils).
Records examined by —.
Purpose —.

[Sample form D]

NOTIFICATION OF TRANSFER OF PERMANENT PUPIL RECORD TO ANOTHER SCHOOL SYSTEM

Dear Parent, You are hereby notified of the pending transfer of (name of pupil)'s permanent school record to (name of school district in (location)).

Should you wish to receive a copy of the record to be transferred please return the bottom portion of this form with your signature by (date).

Sincerely,

_____,
Principal.

I wish to receive a copy of the school record of (Please print name of pupil) who is my (son) (daughter) (legal ward).

Parent's signature and date.

Address to which transcript should be sent:

[Sample form E]

REQUEST FOR PERMISSION TO RELEASE PERMANENT SCHOOL RECORD TO THIRD PARTY

Dear Parent, We have received a request from (name of requesting individual agency, etc.) for a copy of (access to) (name of pupil)'s school record.

Please indicate in the space below whether you are willing for us to comply with this request.

(Name of requesting party) may have a copy of (access to) the following parts of (name of pupil)'s record:

Official Administrative Record (name, address, birthdate, grade level completed, grades, class standing, attendance record).—
Standardized Achievement Test Scores.—
Intelligence and Aptitude Test Scores.—
Personality and Interest Test Scores.—
Teacher and Counselor Observations and Ratings.—
Record of Extracurricular Activities.—
Family Background Data.—
Parent's signature and date.

[From Harvard Educational Review, February 1974]

EXCERPTS FROM AN INTERVIEW WITH MARIAN WRIGHT EDELMAN*

Marian Wright Edelman, as Director of the Children's Defense Fund of the Washington Research Project, has added child advocacy to her agenda of action for social change. Beginning as an attorney in the civil rights movement, she directed Jackson, Mississippi's office of the NAACP Legal Defense and Education Fund, Inc. Headstart, children, and education were large issues for community development, and her involvement with the Child Development Group of Mississippi focused her concern on the welfare of poor and minority children. One of the principal architects of the Comprehensive Child Development Act of 1971, she has broadened her commitment to advocate the rights of all children. She has selected several specific areas on which to concentrate: the exclusion of children from school, labeling and treatment of children with special needs the use of children in medical experimentation, their right to privacy with re-

*Interviewers were Rochelle Beck and John Butler of the HER Editorial Board.

gard to school and juvenile court records, reform of the juvenile justice system, and children's right to day care of high quality. Ms. Edelman talked about about these and other issues with HER.

Marian, you recently announced the formation of a new organization, the Children's Defense Fund. Can you tell us what it is and why it was created?

The Children's Defense Fund (CDF) is an attempt to create a viable, long-range institution to bring about reforms for children. If they are to receive fair treatment and recognition in this country, children require the same kind of planned, systematic, and sustained advocacy, legal and otherwise, that the NAACP Legal Defense and Education Fund, for example, instigated for blacks three decades or more ago. We hope to bridge two large gaps. One is between people in local communities and advocates at the federal level. The former care about kids but have no larger strategies into which they can fit their local action, and the latter may be politically savvy but need support from local groups to implement any kind of change. Professional child advocates may know a great deal about federal legislation and administrative processes, but unless we can transmit such knowledge to local groups who can educate their constituencies and provide the political muscle, we will continue to lose much of our effectiveness.

The second gap is among people in various disciplines. Researchers and academics have gone off in one direction and those of us who have been involved in policy have gone off in another. As a result, there is often no useful evidence on the particular issues policymakers need to make decisions about. I think there is a lack of understanding from the academic community of what we need to know and do for children with immediate needs. Similarly, lawyers have spent a lot of time filing suits and winning legal victories but have not paid adequate attention to the problems of remedy or the involvement of the community. For example, a right to a hearing is hollow unless people know they have it and are helped to take advantage of it.

CDF is attempting to cut down on the usual fragmentation of effort by molding a staff of people from various disciplines who will seek a unified approach to change. We have litigators and researchers, federal administrative monitors, and community liaison back-up people. We have contracted with local organizing groups like the American Friends Service Committee to provide us with eyes and ears sensitive to local people and problems. We are also retaining local attorneys whom we can use to help identify, where possible, those effective local action groups working in behalf of children.

There is also a separate national entity, the Washington Research Project Action Council, which has a legislative agenda and can lobby on behalf of children—with child development and child health legislation at the top of the list.

What are the specific issues CDF has chosen to pursue?

CDF is premised on the assumption that effective advocacy is specialized; global approaches to change on behalf of children are doomed. We have selected six priority issues for change which could affect broad numbers of children and which are easily understood by large segments of the public. They are: One, the exclusion of children from school; two, classification and treatment of children with special needs; three, the use of children in medical, particularly drug, research and experimentation; four, the child's right to privacy in the face of growing computerization and data banks; five, reform of the juvenile justice system, and six, child development and day care. These issues are subject to attack from a number of vantage points—local, state, and federal—as well as through a combination of strategies, such as litigation, monitoring, model legislation, or efforts at exposure which might in turn provoke congressional hearings, local organizing efforts, and so forth.

What are the other priorities for CDF?

One is what we call the "Guinea Pig Project," where we are investigating the extent to which children, particularly institutionalized children, are used for medical experimentation without the provision of adequate informed consent procedures or other protections. It is an extremely interesting area. We have found it difficult for two reasons: First, medical research has been conducted largely in secrecy, without public knowledge of accountability, even while much of it is done with public funds; and second, doctors, like lawyers and other professionals, think that only they should regulate themselves—even in the face of information showing substantial abuse. The Tuskegee syphilis experiment and the South Carolina sterilization case dramatically illustrate the need for public attention in this area.

We recently won an important case in the Federal District Court of the District of Columbia under the federal Freedom of Information Act. This decision allowed us access to NIMH grant applications and research protocols, including so-called pink sheets and site visit reports, which contain the conclusions and comments of peer review groups whose approval is required of all federal research applicants. The Court also ordered HEW to revise its regulations and grant application procedures to assure that such materials are made available to the public in the future. This decision, if sustained on appeal, will go far in demystifying medical research and building some public accountability into federally funded research grants affecting children. Our investigation of the medical practices in this area will result in a report later this year.

It is a sad fact that there is a better government policy to protect animals than children from experimentation. It is only in the aftermath of blatant abuses that government panels have been assembled to discuss and draft more specific guidelines for human experimentation. I am especially concerned about preventing institutionalized children from being used for experimentation. It still remains to be seen when, and in what form, guidelines in this area will emerge. CDF has monitored the guideline drafting process carefully, and we have prepared and are advocating our own draft regulations.

How are the current guidelines for human experimentation insufficient to protect children?

The current guidelines governing human experimentation are inadequate on the informed consent issue. They completely ignore the problems of consent among the institutionalized. CDF's top priority in this area is to safeguard the child who is least protected—the orphan, the retarded, the neglected and dependent, the institutionalized and the poor—from being guinea pigs in the marketing of new drugs. The consent issue is different for adults and children, particularly children who are under the control of the state or third parties. I feel differently about an adult prisoner consenting to participating in a drug experiment than I do about such an experiment being performed on a child in an institution for the mentally retarded or in a home for the orphaned and neglected.

Isn't the notion of consent problematic with children anyway?

Yes. At what age should a child have to be involved in giving consent, rather than simply consulting the child's parent. Should institutions be permitted to give constructive consent for purposes of experimentation? I would not want any jailer in Alabama or elsewhere to have the right to consent on behalf of juvenile wards on such matters.

Whether protections and procedures are implemented is another crucial but difficult issue. Researchers may give lip-service to paper procedures but ignore them in reality. A substantial consent question was raised in an experiment conducted by a Dr. Dimascio through Boston State Hospital.

What was the experiment?

It involved administering drugs to school children in certain Boston public schools who supposedly reflected behavioral problems which were very broadly defined. The early proposal suggested the experiment was more an attempt to test the effect of the drugs rather than a treatment for specifically identified medical problems. The proposal described a potpouri of symptoms such as restlessness or inattentiveness that could have resulted from a variety of social causes like poverty or hunger, as well as from medical causes. Yet the approach in the proposal, apparently directed at poor children, first explored therapeutic rather than social solutions to the symptoms. If a child is restless because he's hungry, adequate nutrition ought to be the first level of inquiry and response—not the administration of some drug. Further, it was unclear, just what the parents were told about the experiment or how the content procedure worked. I know as a parent I would never have consented to my child participating in such a poorly designed experiment. But when we tried to find out more, we were turned down. It was to get this proposal and others that we sued NIMH under the Freedom of Information Act and which resulted in the decision I mentioned earlier.

We have met with a great deal of defensiveness and concern among some of our friends in the medical profession who fear that we are out to (or may inadvertently) destroy medical research. That is the farthest thing from our intentions. We do believe that it is important to enforce public accountability on these important issues. This is an issue which involves very complex judgments, but a total policy vacuum or reliance on self-regulation within the medical profession in the face of increasing evidence of abuse is not a desirable solution.

To give you a specific example, it is necessary, in my opinion, for more people to be aware of and question the frequency with which drugs like Ritalin are employed in the treatment of children's problems. The use of amphetamines on children is far more widespread and promiscuous than has been suspected or documented. And for imprecisely defined medical problems. What is a hyperactive child? How much misdiagnosis is involved? Who should diagnose the child? A physician? A teacher? A parent? What is the impact of long-term use of such drugs? Is the availability of drugs an incentive for easy, maybe incorrect, labels and treatments which serve as substitutes for more costly, complex, or demanding services for children?

You mentioned that a child's right to privacy in the face of growing use of computerization and data banks was a CDF interest. What are you doing in this area?

We have begun what we call our 1984 Project, which focuses on behavioral screening for the purpose of identifying and labeling children with alleged criminal or other behavioral problems and on exploring the use of computerized record keeping of information on children.

This project examines the crucial issues of privacy and classification, to say nothing of raising more fundamental issues about what kind of country we are or ought to be. I have very strong feelings about how much the government or other officials ought to be allowed to know about individuals. Indiscriminate data banking and careless sharing of information can subject those childdren who are most disliked and most prone to be mislabeled—the poor minority child, the neglected child—to unfair scapegoating by governmental authorities. Children may gain a stigma at a very early age that can never be shaken. For example, a young person picked up for speeding at sixteen might be checked through some centralized data bank and found to have a history of school problems or contacts with the juvenile court. He or she will, in all likelihood, be treated differently once this information is known.

Accessibility of school records also presents problems. Some information fed into a child's records (to which she or he may not have had access) may be of questionable nature. For example, suppose a principal or teacher thought the child was on drugs but could not prove it. Suppose this observation was included in a school file which was later turned over to the juvenile court when the child was picked up for truancy. This information might later go into a data bank accessible to police authorities. The ramifications of the unsubstantiated charges could go on and on and the child would never have the opportunity to refute them.

Some say that various kinds of specialists in the schools should have access to all information about the child and use it at their discretion. Others say that this kind of information should be withheld from school personnel and reserved for the parents, unless they want to divulge it, thus arguing for something more like a formal doctor-patient relationship between the specialist and the child. How do you see it?

It seems to me that if there is a counseling service at a school, the counselor should have access to the records necessary to do his or her job. This is true of any specialists attempting to deal with special problems. The information sought and collected, however, should be appropriate and necessary to the service being performed. None of the data should go outside the school, for any purpose, without the parents' or the child's consent (depending on age).

Unfortunately, it is still the practice in many places to deny parents and children access to school records. A new law giving parents access to their children's records was recently passed in Massachusetts. This right does not exist in many other states. Like welfare recipients' records, all files are confidential. Even the person on whom files are kept may not see them. Who is being protected from whom? One of the reasons it's so important to give parents and student access to their own files is to cut down on the hearsay evidence and rumor that often serves as the basis for labeling a child. In instances when a child is on trial, stands to be expended or expelled from school, or otherwise has his status negatively altered in a serious way, his parents and counsel should certainly have access to all information of records upon which the charges were based.

[From the Congressional Record—Senate, May 14, 1974]

EDUCATIONAL AMENDMENTS OF 1974

Mr. BUCKLEY. Mr. President, as more stories come out in the media about the abuses of personal data by schools and Government agencies, the public and Congress have become increasingly aware of the problems such abuses pose. In

addition, the revelations coming out of Watergate investigations have underscored the dangers of Government data gathering and the abuse of personal files, and have generated increased public demand for the control and elimination of such activities and abuses. It is appropriate therefore, that we take this opportunity to protect the rights of students and their parents and to prevent the abuse of personal files and data in the area of federally assisted educational activities.

Many absurd and sometimes tragic examples of similar abuses exist. Let me recount one of the cases described in the recent article, "How Secret School Records Can Hurt Your Child," in Parade magazine:

"The parents of a junior high student are told their daughter won't be able to attend graduation ceremonies because she's a "bad citizen." What has she done that's bad, the parents ask? Well, the principal says, the school had a whole file on her "poor citizenship," but the parent can't know what's in that file. In this Catch-22 case, one of the few to get a legal hearing, the New York State Commissioner of Education, Ewald B. Nyquist, stated flatly that the school's argument that it was acting in the best interest of the student in refusing to reveal the information to the parents—had no merit. The commissioner concluded: "It is readily apparent that no one had a greater right to such information than the parents."

When parents and students are not allowed to inspect school records and make corrections, numerous erroneous and harmful material can creep into the records. Such inaccurate materials can have devastatingly negative effects on the academic future and job prospects of an innocent, unaware student.

Many examples of abuses can be found in recent letters to the National Committee for Citizens in Education which has for a long time carried on the fight for the right of parents to have access to their children's records by alerting and assisting parents across the Nation. I would like to take this opportunity to commend that committee for its dedicated efforts, and to mention that the NCCE will very shortly publish a major study entitled "Children, Parents and School Records." It is must reading for anyone who is concerned with the issue of privacy and the schools.

Violations of the privacy of students and their parents occur daily in schools across the Nation, through courses requiring the student to reveal personal data and feelings, and by means of demands by the Federal Government for personal information on students and parents. The recent refusal of the District of Columbia School Board to refuse to administer a battery of tests, despite a threat by the Federal Office of Education to cut off nearly $6 million in Federal funds to the city' public school system, is a good case in point. The superintendent of the schools, Barbara Sizemore, charged that many items in the tests, which are required in other school districts around the Nation, are a violation of privacy and could cause psychological damage to students.

The New York City School Board refused to comply with a similar demand. Dr. Seymour Lachman, president of the school board, said that the original demand "violated the confidentiality of student records" and that, lacking proper safeguards, the data might be misused or abused. He added that:

"These kids could have been categorized, codified, and stereo-typed for life on the basis of information put on the tape while they were in school."

In addition to being denied access to their children's school records, parents are often unable to readily review the instructional materials in various courses in which their children are enrolled. And often they are not asked to give their consent before their child is given very personal or psychological tests, or participate in experimental programs or attitude-affecting courses.

The secrecy and the denial of parental rights that seem to be a frequent feature of American education is disturbing. Some school administrators and educators seem to have forgotten that parents have the primary legal and moral responsibility for the upbringing of their children and only entrust them to the schools for basic educational purposes.

Some educators seem to feel that they know much more about the welfare and best interests of the child than do the parents, and therefore, once a child comes under their sway, they think they have the right to do what they themselves think is best for the child, without regard for values and beliefs of the parents.

The world-famous child psychiatrist, John Bowlby, noted in an interview concerning the care of young children last year, that:

"The criticizing of parents and taking the children out of the home and putting them into the schools as is being commonly suggested these days actually under-

mines the parental confidence in the parents' own role, and in their potential role. There is entirely too much criticism. The educators are guilty of undermining the home rather than building it up."

There has been an increasing chorus of complaints from parents in the last few years about just such attitudes and actions on the part of some educators. The sense of a loss of control over one's life and destiny, which many social commentators say is growing amongst our citizens, seems to be increasingly felt by parents with respect to the upbringing of their own children.

Such elitist and paternalistic attitudes reflect the widening efforts of some, both in and out of Government, to diminish the rights and responsibilities of parents for the upbringing of their children, and to transfer such rights and functions to the State—to separate, figuratively, and in some cases, literally, the child from his parents, and to turn him over to the care of the State, as represented by schools and other arms of its administration.

My amendment seeks to restore parental rights and to protect privacy. It will:

First, help insure that parents have the right of access to their children's school records;

Second, help prevent the abuse and improper disclosure of such records and personal data on students and their parents;

Third, require parental consent before such records are disclosed to most third parties;

Fourth, require parental consent or notification before their children are made to undergo certain forms of testing or partake in certain experimental or attitude-affecting programs or activities; and

Fifth, make instructional materials used in the classroom available for review by parents upon request.

In addition, my amendment requires the Secretary of HEW to adopt appropriate safeguards to protect the rights and privacy of students and their families in regard to Government authorized surveys and other data gathering activities.

My amendment broadens the protection of civil rights to include the civil rights of parents and students vis-a-vis the schools. As a matter of fact, a recent Federal court decision has made the civil rights aspect of privacy and parental consent more explicit.

The case was Merriken against Cressman, heard in the U.S. District Court of Eastern Pennsylvania last fall. Let me quote from the summary of the case in "The United States Law Week" of October 16, 1973:

[The article follows:]

A school district proposed to use a program entitled Critical Period of Intervention (CPI) for the purpose of identifying potential drug abusers among its eighth-grade students. Additionally, the program would "prepare the necessary interventions, identify resources to train and aid the district personnel to remediate the problems and, finally, to evaluate the results." Parental consent in a prerequisite to a student's participation in the program. Such consent is solicited by a letter which is admittedly a "selling device" and "an attempt to convince the parent to allow the child to participate."

Two child psychiatrists testified without contradiction as to several * * * dangerous aspects of the CPI Program, none of which are mentioned * * * in any of the materials to be made available to parents. These dangers include the risk that the CPI Program well operate as a self-fulfilling prophesy in which a child labeled as a potential drug abuser will by virtue of a label decide to be that which people already think he or she is anyway * * * Another danger mentioned is that of scapegoating in which a child might be marked out by his peers for unpleasant treatment either because of refusal to take the CPI test or because of the result of the test. Additionally, there is a "severe loyalty conflict that might result by asking children the types of personal questions about their relationship with parents and siblings which are included in the CPI questionnaire." Finally the qualifications of the school district personnel who will administer the interventions once potential drug abusers have been identified are woefully inadequate.

The court found that the confidentiality of the program broke down when the school superintendent was informed of the potential drug abusers, who were then required to undergo attempted psychological remediation by ill-trained faculty members. But, said the Judge:

"The ultimate use of this information, although possibly gained with a great deal of scientific success, is the most serious problem that faces the Court. How many children would be labeled as potential drug abusers who in actuality are not, and would be subjected to the problem of group therapy sessions conducted by inexperienced individuals?

"Strict confidentiality is not maintained after evaluation and there are many opportunities for a child to suffer insurmountable harm from a labeling when the cruelty of other children is at an extreme. The seriousness of this problem is illustrated by the fact that if one child is so harmed and would be temporarily or permanently damaged by the label of 'drug abuser,' is this Program worth the effort to identify other actual 'drug abusers.'

"When a program talks about labeling someone as a particular type and such a label could remain with him for the remainder of his life, the margin of error must be almost nil."

The court found that the potential for harm of this program outweighed any good that might accrue, and concluded as a matter of law that the CPI program violated the right of each student and his parents to privacy inherent in the penumbra of the Bill of Rights of the U.S. Constitution.

This case is a microcosm of the problems addressed by my amendment—the violation of privacy by personal questionnaires, violation of confidentiality and abuse of personal data—with its harm to the individual—and the dangers of ill-trained persons trying to remediate the alleged personal behavior or values of students. It describes the potential harm that can result from poorly regulated testing, inadequate provisions for the safeguarding of personal information, and ill-devised or administered behavior modification programs.

In fact, it shows that even the requirement of parental consent can be an inadequate safeguard in the face of the slick and deceptive selling techniques of some educators. Yet, at least the requirement of parental consent informs the parents, to some extent, about what is being done with and to their children in schools, and it offers the best available protection against educational abuses that I can think of. Additionally, it will encourage schools to improve these types of programs and to eliminate the potential for abuses beforehand, thereby tending to reduce the future occurrences of irate parents going to court because of shoddy and harmful programs in the schools.

If anyone doubts the seriousness of the problem, I direct their attention to a recent communication from the National Education Association (NEA) in which that organization announced its opposition to my amendment which would require school officials to obtain prior, written, informed consent whenever the school officials would have those parents' children subjected to a project, program or course, the primary purpose or principle of which is to affect or alter the personal behavior or personal values of a student. Mr. President, I would like to point out the implication of the NEA's position. It is their position that as between the parent and the school official, the latter has the more fundamental right to determine whether the child should be subject to program of behavior alteration and value modification.

Beneath such a position is a very serious threat to the traditional notion long respected by this Nation that it is the parents who are ultimately responsible for the welfare of their children. It borders on shocking that one of the national organizations representing educators would move to have the Senate oppose a reaffirmation of this important and real parental right. Further, the attempt to characterize the amendment as one which intends to curtail freedom of expression between child and teacher is incredible. It is more accurate to conclude that it is the NEA's position that the teacher should come between parents and child on such important matters as school programs, the primary purpose at which is behavior modification and values alteration.

I would respectfully suggest, Mr. President, that the burden to secure consent of the parent is not too great. Surely, most conscientious teachers would have no problem gaining the consent of a parent providing the teacher has demonstrated the worth of his proposal. To suggest otherwise is to insult the parent and underestimate the resources of America's educators.

Some may argue that my amendment will create too much additional work and redtape for schools and the educational bureaucracy. To that argument I must reply that I am not so much concerned about the workload or convenience of the educational bureaucracy but, rather, with the personal rights of America's children and their parents. I believe that their rights should properly take such priority in whatever educational legislation the Senate, in its wisdom, shall enact.

It has been argued that portions of my amendment would throttle innovation and virtually close down title III and other innovative educational efforts sponsored by the Federal Government. This is surely not the intent of my amendment, nor would it be the effect. My amendment simply gives individual parents the right to be informed about out-of-the-ordinary federally funded programs in which their child might participate, and assures the parents the right not to have their particular child participate if they find such a program objectionable. Granted that there will be some inconveniences and logistical problems involved in this. But what sufficient reason is there for anyone to stand up and say that parents must be denied these rights? What do the schools and the Federal agencies have to hide?

As a matter of fact, my amendment need not create undue problems. For example, the Russell Sage Foundation published a very thoughtful study in 1969 entitled, "Guidelines for the Collection, Maintenance, and Dissemination of Pupil Record," which included samples of simple forms that could be mailed to parents to obtain their permission for certain activities with regard to their children. I would also further note that many schools and a number of States already routinely require the prior consent of parents on a number of matters, including both special testing and some special programs or projects, such as drug programs or sex education.

Permit me to add, also, that many elements of my amendment follow the recommendations of the report of the Secretary's Advisory Committee on Automated Personal Data Systems at HEW, entitled "Records, Computers, and the Rights of Citizens."

Equally important as the other effects of my amendment is the likelihood that the obligation to inform parents will begin to close the gap of hostility that too often exists between parents and teachers, each distrusting the other. The increased openness and communication with parents on the part of the schools which would follow from my amendment would enhance parental interest and involvement in their children's education, and in the long run could lead to improved education and more harmonious school-community relations.

Mr. President, it is time for the U.S. Senate to take a stand in favor of, and to act to protect the rights and privacy of parents and students where the Federal Government and Federal funds are involved. Therefore, I urge the Senate to give favorable consideration to my amendment.

I reserve the remainder of my time.

Mr. MATHIAS. Mr. President, will the Senator yield?

The PRESIDING OFFICER. Under the unanimous-consent request, the Senate must return to consideration of the Javits amendment.

Mr. JAVITS. I yield myself 2 minutes on the bill.

After discussion with Senator Pell, I wish to state the following facts: One, Puerto Rico is treated as a State in the House, so the amendment will be in conference. Two, we should figure out exactly what the relationship would be of the poor children who would be covered in Puerto Rico, which we will do, compared to the other States, and see, therefore, whether my estimate of something a little more than 2 percent, but not substantially over that, is justifiable. I want to check that out. Three, I now ask the Chair to make a ruling on this: Notwithstanding the fact that a substantive question may be affected, an amendment may occur at a later part of the bill, notwithstanding the adoption, if it should be adopted, of the McClellan amendment, which may make a substantive change, provided it does not cover the same language which is contained in the McClellan amendment—whether another amendment, under the rules of the Senate, would lie at the end of the bill.

The PRESIDING OFFICER. So long as the amendment is redrafted, so long as it does not affect the text of the amendment, it would be in order.

Mr. JAVITS. Under those circumstances, Mr. President, I withdraw the amendment.

The PRESIDING OFFICER. The amendment is withdrawn.

Mr. MATHIAS. Mr. President, will be Senator yield?

Mr. PELL. Mr. President, we are on the Buckley amendment, with how much time on each side?

The PRESIDING OFFICER. The McClellan amendment is before the Senate at the moment. A unanimous-consent request would be in order to proceed to the Buckley amendment.

Mr. ROBERT C. BYRD. Mr. President, I ask unanimous consent that the Senate now proceed to the consideration of the Buckley amendment, No. 1289.

The PRESIDING OFFICER. Without objection, it is so ordered.

Who yields time?

Mr. MATHIAS. Mr. President, will the Senator from New York yield me 3 minutes?

Mr. JAVITS. Yes, in opposition.

Mr. MATHIAS. I have some questions I would like to ask the distinguished junior Senator from New York, because I salute the thrust and the purpose which I think he seeks to accomplish by this amendment.

But I do want to be perfectly certain that I understand the practical effect of it. Turning to section 437(b)(1), page 3, I am wondering what effect this provision would have in the case of a student who was the victim of an accident in the school, or the victim of an accident on a playground. Would it prevent the school from arranging to have him immediately examined and medical treatment given to him?

Mr. BUCKLEY. No, of course not. Normal medical advice and hospital procedures usually require parental consent, and in those situations where the parents could not be contacted the treatment would be available.

Mr. MATHIAS. Would it not be necessary then, to have an exception because there is an exception in the general immunization, and I think the case of emergency treatment would have to be made in an excepted case or else the school would be under some jeopardy here.

Mr. BUCKLEY. I would be glad to ask unanimous consent to amend my amendment by inserting on line 11, page 3, following the word "immunization" the words "or emergency medical treatment."

The PRESIDING OFFICER. Is there objection to the Senator from New York modifyling his amendment to that effect? The Chair hears no objection, and it is so ordered.

Mr. MATHIAS. If there were a course being given which is clearly a course which is causing the student to alter his behavior for the good, let us say in the matter of grooming, as the result of a course in civics, where he has become more interested in the system, and we have a course which is a positive influence on the student's life, would the Senator's amendment require the parents' "prior, informed, written consent" for that type course?

Mr. BUCKLEY. Quite obviously in one sense all education has an effect on attitudes, and so forth. I believe there is a tacit rule of commonsense that applies to the interpretation and application of all legislation and I speak of courses, the primary purpose of which is to modify behavior.

The PRESIDING OFFICER. The time of the Senator from Maryland has expired.

Mr. MATHIAS. Will the Senator yield to me for 3 additional minutes?

Mr. PELL. I yield.

Mr. BUCKLEY. So clearly the example of the Senator from Maryland would not be covered.

Mr. MATHIAS. Of course, my concern is that the language of the amendment might cover it. That is what gives me some uncertainty.

Let me pass to section 437(c)(1). Let us assume the unhappy possibility that a student is suspected of having bombed the chemistry laboratory and the FBI or another law enforcement agency comes into the school, let us say, without a judicial order. Would they be unable to examine the records or files of the student without the "prior, informed, written consent" of the student's parents?

Mr. BUCKLEY. I believe they should get a court subpena to have access to the records.

Mr. MATHIAS. The amendment does not even provide for access with a subpena without parental consent.

Mr. BUCKLEY. I refer to page 6, where it is stated:

In compliance with any court order, or pursuant to any lawfully issued subpena, if the parents and students are notified of any such order in advance of the compliance therewith . . .

Mr. MATHIAS. The Senator is correct but also it would require the warrant or the written consent, even in the case I suggested.

Now, I wish to ask the Senator this question. Does the provision allow the use of any identification device other than the names of students or the names of parents?

Mr. BUCKLEY. No, it does not.

Mr. MATHIAS. So that would be the only possible identification, there could be no other identification of any sort?

Mr. BUCKLEY. No.

Mr. MATHIAS. And the Senator feels that that is a useful provision.

Finally, there are certain programs in which there is some testing, specifically, HEW through the National Institute of Education has made a grant to test and experiment with an educational voucher program. I am sure the Senator is familiar that such programs are now underway in California and Vermont.

Under this provision if the parents of a child object to the child's participation, then that child would not be able to take part. Is that correct?

Mr. BUCKLEY. That is correct.

Mr. MATHIAS. What will happen to a program of that sort.

The PRESIDING OFFICER. The time of the Senator from Maryland has expired.

Mr. MATHIAS. Mr. President, will the Senator yield to me for 1 additional minute?

Mr. PELL. I yield 1 additional minute to the Senator from Maryland.

Mr. MATHIAS. What will happen to that child if the entire school is involved? What happen to that child when the whole school is involved, as in the case of California and Vermont? Does the child have to be withdrawn from that school and some alternative education provided?

Mr. BUCKLEY. That child would obviously be handled in the school as if he were not—in other words, his State directly would pay for that tuition.

Mr. MATHIAS. Then, the Senator's concept is that under this provision——

Mr. BUCKLEY. It would not abort the experiment.

Mr. MATHIAS. But the child would have to have some other education provided in some other location or in some other manner.

Mr. BUCKLEY. If a parent did not want to accept the voucher the child would continue to be educated in the school he attended.

Mr. MATHIAS. But if the whole system were committed to the program, there would be no other school for him to attend. That seems to be the nub of the problem.

Mr. BUCKLEY. I disagree. I do not believe it would be interpreted in that way.

The PRESIDING OFFICER. Who yields time?

Mr. PELL. Mr. President, the junior Senator from New York and I have previously discussed this amendment. I ask unanimous consent that a letter from the National School Boards Association be inserted in the Record.

There being no objection, the letter was ordered to be printed in the Record as follows:

NATIONAL SCHOOL BOARDS ASSOCIATION,
Evanston, Ill., May 2, 1974.

Hon. CLAIBORNE PELL,
U.S. Senate, Old Senate Office Building, Washington, D.C.

DEAR SENATOR PELL: Pursuant to his "dear colleague" letter dated April 26, 1974, Senator Buckley set forth proposed amendments to S. 1539 relating to "Protection of the Rights and Privacy of Parents and Students" (Sec. 513). In general, the National School Boards Association believes that the intent of the amendment is meritorious, but that operationally its accomplishment will generate unacceptable confusion because of the complicated legislative language and local administrative conditions associated with the approach taken in the amendment. We have been in contact with the Sentaor and he has some of our specific concerns under advisement. Those concerns are outlined below:

1. The amendment requires that parents have the right of access to their child's school files and that their consent be obtained prior to release of such files to third parties (with certain exceptions). However, if the rights of the students are distinguishable from the rights of parents, and if the assertion of those rights should not be solely dependent upon parental willingness, the amendment should give students an independent right of access to, and consent with respect to the divulgence of, their files. At the same time, it may be advisable to impose a minimal age, such as 15 years, at which the child's independent rights would attach.

2. The amendment requires that school authorities provide parents with student files within thirty days after the request is made. In many instances, records may have to be screened in order to delete references to third persons, or the records sought may be stored in a central school district file or at the state level. Accordingly, while administrative footdraging cannot be condoned, compliance in many instances will not be possibe unless the time limit is extended to 45 days—and preferably 60 days.

3. Subsection (b) of the amendment provides that no student "participating in an applicable program" shall be required to undergo medical, psychological, et cetera, examinations without parental consent. This means that if a state or local

agency is operating an examination program of that kind and is not receiving federal aid, consent is not required. But if the education agency is receiving ESEA II library funds, for example, then consent is required. The basis for this distinction is difficult to understand. Since the examination in question would be pursuant solely to a state program authorized and perhaps mandated by state law, federal legislation would be inappropriate in either case as a matter of policy. However, a different situation *may* arise when the education agency includes such an examination as *part* of one of its federal programs. If the latter situation is a proper area for federal involvement, then the overbreadth of subsection (b) (1) can be corrected if, after the words "no student" the words "participating in" are deleted and the words ", as a part of," are substituted in lieu thereof.

4. Subsection (b) of the amendment also prohibits the participation of any student in an applicable program which involves *any* research or experimental project without the consent of the student's parent. Research and experimental project is then defined as "includes but is not limited to, any program or project designed to explore or develop new or unproven teaching methods of techniques, or to explore or develop teaching techniques or courses affecting the social development, personal behavior, or values of the student." Given the broad brush of the above definition, quite conceivably almost any classroom effort would be subject to challenge on the grounds of "new" pedagogical style or personal impact upon particular students. But even at some point short of a literal application, the above definition will grind public education into a stultifying routine rather than the creative experience which it should present for children. And, to the extent any innovation is challenged there is some question whether the Department of Health, Education, and Welfare will make nationally or community based judgments as to new techniques or definitions of student values. In either case it is also questionable whether the federal government can or ought to be involved in deciding questions relating to "social development, personal behavior, or values of the student." The requirement of individual parental consent to all programs raises other questions of federal policy. We now have federally mandated state advisory committees, local advisory committees, and even in some programs, school by school parental committees. That amendment adds yet another layer to the existing stream of administrative costs and formalities associated with school board policy implementation. One might begin to ponder the role of the taxpayer voter in our education system after one more review is added on top of the governmental structure which he elects to represent him. Although this restriction only applies to federal programs (which in itself is perplexing, inasmuch that if restrictions on experimentation is the object sought, the source of funds should be irrelevant), that to is overboard. If such a restriction is really advisable, it should only be applied to ESEA Title III programs, which are designed for experimental purposes, and not to programs such as ESEA Title I or NDEA III, which are not intended to expose the child to innovative techniques on other than a random or incidental basis.

5. Subsection (c) requires parental consent for the release of personal data, except in certain instances, including the "order of administrative agencies having the power of subpoena." It would appear that a federal agency, which is so empowered can by-pass the amendment merely by issuing a general order applicable to all students who, for example, attend a particular school, are involved in particular activities, etc. While investigations by federal officials may be necessary in certain circumstances, if the scope of the above exception is as broad as we suggest, then the basic purpose of the amendment is defeated.

6. Subsection (c) (4) of the amendment requires that a list of all persons or agencies desiring access to a student's records shall be maintained in that student's file. Although parents, students, and *certain* school officials should have access to that list, other persons or agencies should not—lest the student be characterized by the innuendo of previous searchers of his files.

It should be mentioned that the financial costs of producing records, implementing parental consent procedures for innovation and divulgence of information, and maintaining information requests lists are subordinate to the primary objective sought by the amendment—but should be taken into account nevertheless. Unfortunately, we do not have ample time to develop cost figures.

In summation, we urge that you withhold support for the amendment, unless the above described problems are resolved.

Sincerely,

AUGUST W. STEINHILBER,
Assistant Executive Director, Office of Federal Relations.

Mr. PELL. Mr. President, I am not enthusiastic about the amendment, but it does have some merit. Section (b) concerns me.

The amendment disturbs me in that it states that:

No student shall be required to undergo . . . testing without prior written consent of the student's parents in any project.

The thought I have is that if the Senator would withdraw that section (b), we could decide the fate of his amendment by voice vote, and my voice would be saying "aye" or if he insists on leaving it in, which from my side of the aisle I do not recommend, I would have to ask for a rollcall vote.

Mr. JAVITS. Mr. President, will the Senator yield?

Mr. PELL. I yield.

Mr. JAVITS. Under these circumstances the amendment could be taken to conference, but the administration has grave problems with other parts of it. Having reviewed the administration's wishes, I believe they would be susceptible to handling it in conference. However, I do not want my colleague to feel we have written letters of love that we are going to preserve all of it. I think the administration's suggestions do not change its fundamental thrust, but takes certain precautions. I hope in conference we can work it out that way.

Mr. STEVENS. Mr. President, will the Senator yield?

Mr. PELL. I yield.

Mr. STEVENS. Mr. President, I have serious questions about subsection (c) which I think runs contrary to a great many Federal policies and the best interests of the student. I intend to offer an amendment to either delete that section or to modify it substantially in several ways. I just want to let my friend from Rhode Island realize that. I hope to have a chance to have an exchange with the Senator from New York concerning that.

As I understand subsection (c), it would prevent a high school from giving to a bank that wants to send out information about its loan program to students, the names and addresses of students without consent of the students' parents. I cannot understand this overprotectionism to the point that it could not offer to those students information about Federal loan funds. One could not get the names and addresses of students in ones' State to get them the information of the opportunities available under the Federal student loan program.

Under subsection (c), if I were a probation officer, I could not sit down and talk with the teacher to get personal information from the teacher about the student who was subject to a criminal process. I do not know whether the Senator realizes how many cases go through the juvenile courts these days, but it is a fantastic number.

So I hope the Senator does not think this is going to breeze through without any debate.

Mr. BUCKLEY. Mr. President——

Mr. PELL. Mr. President, I yield to the Senator from New York, on his time.

Mr. BUCKLEY. Mr. President, I believe that argument is a paper tiger. We are talking about invasion of personal, private data. My amendment does not affect matters of public record, which may be names and addresses of people who happen to be students in a school.

Mr. STEVENS. Let me read from subsection (c):

"Permitting the release of records or files (of personal information contained therein) of students without the written consent of their parents to any individual, agency, or organization . . ."

Does the Senator interpret that to mean a bank could not say, "Give me the names and addresses of your graduating seniors?" Does the Senator interpret that to mean a probation officer could not get information from teachers or the files that would help a juvenile accused of a crime?

As prosecuting attorney, I can tell the Senator that probation officers need such information to help the students. I think this is a shotgun approach. I applaud the Senator's desire to protect students, but we are overprotecting in this way with regard to many activities in a school. I do not want to hurt any student, but we are not going to be able to help him with this amendment. That is the trouble with it.

Mr. BUCKLEY. I believe the parents have as much interest in protecting their child as does the Senator from Alaska, but the Senator is reading into the amendment the inclusion of the simple listing of names and addresses in a student's records and files.

Mr. STEVENS. I am happy to know that, but how does a probation officer go about getting that information? I saw a lot of probation officers as district at-

torney. If they were to have to go to busy juvenile court judges and subpena that information, or if they want to talk to teachers, they are not going to get it. I do not see the necessity for subsection (c). What is the necessity for it?

Mr. BUCKLEY. I described it in my statement. The fact that this information gets leaked out all over the place is injurious to the child. It haunts children in their later lives. I think we ought to put a stop to it.

Mr. President, how much time do I have remaining?

THE PRESIDING OFFICER. The Senator has 18 minutes remaining.

Mr. BIDEN. Mr. President, will the Senator yield me some time to ask the Senator from New York some questions?

Mr. BUCKLEY. Mr. President, I yield 5 minutes to the Senator from Delaware.

Mr. BIDEN. The Senator from New York, I think, should be complimented on this amendment. I think it is long overdue. I do not share the concerns of the Senator from Alaska. Having been a public defender, I do not think a probation officer should be able to sit down and talk with teachers about these matters. They think they are psychologists and psychiatrists, and they do more harm to the child than they help him. But my objection relates to subsection (b).

I am early cosponsor of this amendment, but I think subsection (b) should be clarified so we understand what it would do. In that section it says:

"No student shall, as a part of any applicable program, be required, without the prior, informed, written consent of the student's parents, to participate in any project program, or course, the primary purpose of principal effect of which is to affect or alter the personal behavior or personal values of a student, or to explore and develop teaching techniques or courses primarily intended to affect such behavior and values."

If that were to be misread, it could be a very, very restrictive section.

I would like, for the record, to ask a few questions.

Specifically, in a school for the deaf, will a project designed to test the effectiveness of a new audiology machine be termed "research and experimentation" under this amendment?

Mr. BUCKLEY. Certainly not. This is directed toward developing new, experimental educational techniques. Certainly, new devices for helping—it is really a medical device—the deaf to hear, or new research involving such things as "new math" traditional courses—would not be affected at all by this amendment.

Mr. BIDEN. Would diagnostic tests given to students at the beginning of a course in order to gage the strengths and weaknesses of students in various academic disciplines be considered "research"?

Mr. BUCKLEY. No; this is normal research; it is not experimental. It is not research into new research activities.

Mr. BIDEN. So it is not intended to really alter the traditional academic disciplines? The Senator is not going after that?

Mr. BUCKLEY. That is correct.

Mr. ERVIN. Mr. President, will the Senator yield?

Mr. BUCKLEY. I yield.

Mr. ERVIN. This would prevent schools from making guinea pigs out of children and delving into their personal attitudes and their attitudes toward their families, as has been done in many schools throughout the United States. Is that correct?

Mr. BUCKLEY. Yes.

Mr. ERVIN. It is designed to prevent disclosure, except to those who are authorized to receive them, of personal data about these children. Is that correct?

Mr. BUCKLEY. The Senator is correct.

Mr. ERVIN. I am personally in favor of the proposal.

Mr. President, I am pleased to cosponsor the amendment concerning right to privacy and school records proposed by Senator Buckley to S. 1539, the Elementary and Secondary Education Amendments of 1974. The issue of rights to privacy of public school pupils and their parents is one which has recently become highly publicized in many different circles, but it is a problem that has long been with us. The time has come to do something about it.

This amendment would accomplish several worthy objectives. It would give parents of public schoolchildren the right of access to their minor children's school records. Importantly, parents would be able to challenge any part of the contents of the records for their authenticity. The only person having access to those records in addition to the parents would be school officials, the board of education, and officials at a school to which the pupil might be transferring. In order for any other person to have access to the records, the parents must give

their written permission and the permission form would then become a part of the student's permanent record. In addition, no student could participate in any medical or psychological testing program without the prior, informed, and written consent of his parents. Parents of the pupils would be able to review any and all instructional materials that are used by their child's teacher.

One of the primary aspects of this new legislation is the provision stating that the schools, through the board of education, the principal, or the teacher, would bear the burden for informing the parents and students of their rights and for keeping them fully posted at all times of anything that would come within the scope of this legislation. The penalties for noncompliance with this act would be a loss of the Federal funds that had been made available to the school.

Much of the controversy concerning these school records centers around the use of classroom questionnaires that are financed by governmental grants, often the Department of Health, Education, and Welfare or a smilar agency at the state or local levels of government. These questionnaires are thinly disguised as "research projects," although in actuality they often amount to highly objectionable invasions of the psychological privacy of schoolchildren. Oftentimes, the students are told that the responses they give are classified and will not be used for any other purpose than to gather and analyze statistical data on the educational situation in the public schools. However, it has been too often demonstrated that these data stand strong possibilities of being incorporated into computerized data banks or in other ways being disseminated to persons not connected with the educational process.

The questionnaires usually cover many aspects of the student's personal life and personality. The categories cover the student's attitudes toward his home and family, his school and teachers, his feelings about himself, and his feelings about his peers and classmates. It is my belief that no governmental agency has any business conducting such inquiries unless the parents of the children are made fully aware of the subject matter of the inquiry and subsequently give their full consent. The situation now is that children are rarely given a free and unprejudiced choice of answering or not answering the questionnaires. In addition, parents would be able to request to review their children's school records and would have the right to challenge any adverse content.

Mr. President, I intend to ask soon for unanimous consent that some of these questionnaires and summaries of questionnaires be reprinted in the RECORD. However, I do wish to read, for purposes of emphasis, some of the more offensive questions although they are all certainly in that category. The example that I use are from public schools in the States of Maryland and New Jersey, although there exists strong evidence that these unfortunate practices know no geographical boundaries. Practically all of the questions can be answered with a yes or no or multiple choice answers. There is no room for explaining an answer:

HOME AND FAMILY SITUATION

Are you an important person to your family?
Would you like to run away from home?
Are your parents strict or lenient?
Do you often argue with your parents?
What types of appliances, books, furnishings, and leisure facilities do you have in your home?

SELF-EVALUATION

Do you admire students who are bright?
Can you give a good talk in front of people?
Do you wish you were a different child?
Do you feel lonely very often?
Are you one of the last to be chosen for games?
Do you like being just what you are?

SCHOOL AND TEACHERS

Are some students favored over others by your teachers?
Do most other students want to go to school?
Who are your three best friends (complete names)?
For what reasons have you been scolded in class?

How do you rate your teachers to other teachers at your grade level?
Do you ever miss school or a class simply because you do not wish to go?
Does a diploma from your school mean that you behaved yourself or that you really learned something?

PEERS AND CLASSMATES

Do you have many friends?
Does being with other children bother you?
Is it easy for you to make friends?
Do other children get you into trouble at school?
Would you rather play with friends who are younger than you or older than you?

I certainly believe that this is most important legislation and that the Congress should act wisely and in a forthright manner to recognize the rights to privacy of public schoolchildren and their parents. I am particularly impressed by the strong bipartisan support that this amendment has received from members of Congress and from many public and private sectors of our society. I urge the Senate to adopt this Buckley amendment to the Elementary and Secondary Education Act of 1974.

In my mind school officials should not be allowed to maintain any records outside of the reach of parents, much less records of such a personal nature as those we have seen. A parent has every right to know exactly what information is being collected concerning his children, and the provisions of this amendment constitute what I feel are minimum considerations in the protection of that right. While the measures provided for are strong, I feel the seriousness of the issue well justifies the approach. The parent must have ultimate responsibility for the well being of his children. This amendment recognizes that responsibility.

Mr. President, I ask unanimous consent that the questionnaire from the Hackensack Public Schools of Hackensack, New Jersey, be submitted for reproduction in the RECORD. In addition, I ask unanimous consent that the transcript of a press conference held on April 19, 1974, by an organization known as Parents Who Care, based in Wheaton, Md., which recounts this problem in greater detail also be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

HACKENSACK PUBLIC SCHOOLS,
Hackensack, N.J.

LEARNING EXPERIENCE MODULE—FANNY MEYER HILLERS SCHOOL

STUDENT ATTITUDE INVENTORY

Name _____
Boy_____ Girl_____ LEM_____ Grade_____
Date _____

Directions: Listen carefully to each question and decide how you think and feel. If you don't understand a question, ask about it. Answer each question by drawing a circle around either "yes" or "no".

Responses

Attitude Toward Home and Family: yes, 5; no, 3.
Attitude Toward Peers: yes, 5; no, 6.
Attitude Toward Self: yes, 12; no, 9.
Attitude Toward School and Teachers: yes, 13; no, 6.

SCHOOL AND TEACHERS

(Yes or No Answers)

1. Are your teachers interested in things you do at home?
2. Do your teachers give you work that is too hard?
3. Is the LEM a happy place for you to be?
4. Do you like to read at school?
5. When you don't understand something, are you afraid to ask your teacher?
6. Do you like to paint pictures at school?
7. Do you like to write stories at school?

8. Does your teacher help you with your work when you need help?
9. Do you like doing arithmetic problems at school?
10. Do you wish you were in a different class that was not in LEM?
11. Do you like to learn about science?
12. Does the LEM have too many rules?
13. Do you always have to do what the other children want to do?
14. Do you like the other children in the LEM?
15. Do your teachers like some children better than others?
16. Do other people at school really care about you?
17. Are you proud to be in the LEM?
18. Do you often get a chance to make decisions with others in your group?
19. Do you tell people that you like the LEM?

SELF

(Yes or No Answers)

1. Do you often get sick at school?
2. Can you give a good talk in front of people?
3. Do you wish you were younger?
4. Do you wish you were older?
5. Do you often feel happy in school?
6. Are you a good reader?
7. Do you wish you were a different child?
8. Can you wait your turn easily?
9. Are you good in your schoolwork?
10. Are you a good child?
11. Are you one of the last to be chosen for games?
12. Do you feel lonely very often?
13. If you have something to say, do you usually say it?
14. Do you like the teacher to ask you questions in front of the other children?
15. Do the other children in the class think you're a good worker?
16. Do you find it hard to talk to your group?
17. Are most children able to finish their schoolwork more quickly than you?
18. Do you often act silly just so people will pay attention to you?
19. Do you like most of the people you know?
20. Can you be depended on?
21. Do you like being just what you are?

PEERS

(Yes or No Answers)

1. Do other children get you into trouble at school?
2. Do you have to do what the other children want to do?
3. Do you like the other children in the LEM?
4. Do other children in the LEM like you?
5. Do you always let other children have their way?
6. Do you have many friends?
7. Are other children often mean to you?
8. Do your friends usually do as you say?
9. Does being with other children bother you?
10. Is it easy for you to make friends?
11. Would you rather play with friends who are younger than you?

HOME AND FAMILY

(Yes or No Answers)

1. Are you an important person to your family?
2. Do you have certain responsibilities at home?
3. Do you tell your family when you are mad at them?
4. Would you like to run away from home?
5. Is it pleasant to stay at home on days when there is no school?
6. Do you get upset easily at home?
7. Do brothers and sisters prevent you from being happy?
8. Do your parents think school is important?

STATEMENT BY A COALITION OF CONCERNED PARENTS FROM EIGHT MARYLAND COUNTIES REPRESENTING FIVE CITIZENS ORGANIZATIONS ON INVASION OF PRIVACY BY MARYLAND PUBLIC SCHOOLS

Good Morning: My name is Malcolm Lawrence. I am Director of Public Relations for Parents Who Care, a Montgomery County citizens group founded in October 1971. In addition to the Parents Who Care group, I speak today on behalf of individuals from seven other countries in Maryland representing four other citizens organizations.

I should like to introduce the other members of the group.

Mrs. Jean Carter, from Howard County, representing Citizens Advocating Responsible Education (CARE).

Mrs. Pat Dunlap, from Prince Georges County, representing Citizens for Community Schools (CCS).

Mrs. Margaret Kuhn, from Prince Georges County, representing Guardians for Traditional Education.

The remaining individuals represent the Maryland Committee for Public Disclosure in Education; they are:

Mr. James E. English, from Allegany County.

Mrs. Gloria Donohue, from Anne Arundel County.

Mrs. Betty Fahey, from North Baltimore City.

Mrs. Isabel Fox, from West Baltimore City.

Mrs. Rita Ann Ayd, from Baltimore County.

Mrs. Jo Ann Spriggs, from Carroll County.

Mrs. Barbara M. Morris, from Howard County.

I have a statement to make, following which we shall be happy to entertain questions.

The United States Constitution guarantees to the American citizen a number of fundamental rights that can not be infringed by the federal or state governments without compelling justification. These rights include the right to marry, the right to bear children and to maintain a family, the right to control one's own body, and the right to direct the upbringing of one's children.

The essence of these rights is that they are so basic to personal liberty that they merit a high level of protection from invasions by the state. The rights we have cited are sometimes described as "fundamental" or "natural" rights inherent in American tradition or Western values; sometimes they are based upon the 14th Amendment's guarantee of liberty or the 9th Amendment's reservation of rights to the people; in other cases such rights are based on common law principles. Whatever the basis, it is clear that parents, as part of their right to raise a family, retain basic decision-making authority and responsibility concerning their children's education that cannot be abridged by the states whether by direct exclusion of the parents or by indirect exclusion through the withholding of crucial information about their children.

We have called this press conference today to express publicly our strong objections to materials and practices in the public schools of the State of Maryland which we feel constitute invasions of privacy of both students and parents. It is our view that many teachers are similiarly in opposition to these materials and practices, but are unwilling to openly denounce them for fear of reprisal or dismissal from the public school system. We are urging the Governor of Maryland to take immediate steps to safeguard the rights of students, the parents, and the teachers.

Our leading candidate for removal from Maryland public schools is an extensive questionnaire which has just been given to more than 7,000 students in Howard County. The questionnaire was given as part of a research project administered by the Center for the Social Organization of Schools at Johns Hopkins University, funded by a $200,000 grant from the National Institute of Education of the Department of Health, Education and Welfare (Contract No. NE–C–00–3–0114). Last year 7,200 students in grades 4, 5, 6, 8, and 11 were surveyed. This year, between February 1 and March 15, the same students were given a follow-up survey. For each class tested, a team of trained administrators from Johns Hopkins University marched in; the teacher was asked to leave the class; and the students were handed a 17-page questionnaire and told, "This is not a test. There are no right or wrong answers. Your answers will not be given to your teachers or anyone who knows you."

According to a December 1973 report of the Center for Social Organization of Schools, that Johns Hopkins study is designed to "investigate the effects of open

environment schools on student reactions to school life, student self-reliance, student ability to make realistic judgments, and student achievement on standard tests of academic performance." A January 14, 1974 memorandum from the Howard County Superintendent of Schools to Directors, Supervisors, and Principals reported that three evaluating teams will operate in Howard County schools this year: the fifth year of a program being conducted by the University of Maryland, the project of Johns Hopkins University, and a study of the entire school system to be undertaken by the Institute of Field Studies of Columbia University. The Columbia study was described as a survey of data produced by the Maryland and Hopkins surveys, with the purpose of synthesizing these and other findings to come up with "recommendations for future development of the school system."

Three weeks ago, representatives from our groups called on the National Institute of Education to obtain more information on the scope of these projects and to learn where else these programs were either being undertaken or envisaged. The spokesman for the NIE did not shed any further light on the Johns Hopkins survey and refused to respond to the question as to whether NIE was also financing the University of Maryland and Columbia University projects.

I should like at this point to give the substance of a number of questions from the Johns Hopkins University survey. We have divided the questions into three general categories: 1) Family Situation, 2) Self-Evaluation, and 3) Feelings and Attitudes toward the School and Teacher:

First, Family Situation:

The student is asked how most decisions about him are made in the family.

How much a part he plays in the decisions.

How far in school his father went.

How far in school his mother went.

Whether his parents are strict or lenient.

If his parents want him to follow their directions even if he disagrees with their reasons.

Whether his parents often worry that he is up to something they won't like.

Whether his parents disapprove when he disagrees with them in the presence of their friends.

The student is asked whether he knows why he is supposed to do what his parents tell him to do.

Whether he has a lot of loud arguments with his parents about their rules and decisions regarding his activities.

And whether his parents treat him more like a little kid than an adult.

The student is asked if his parents have definite rules relating to the following activities:

The time to be in at night on weekends; the time to be in on school nights; time spent watching television; going around with certain boys; going around with certain girls; eating dinner with the family; using the telephone; clothing; hairstyle; church attendance; household chores; returning home from school; smoking; age for starting to date; going steady; and frequency of dating.

The student is asked to answer YES or NO as to whether the following items are in his home: Telephone; two telephones; vacuum cleaner; stereo hi-fi record player; air conditioner; electric dishwasher; your own family washing machine; your own family clothes dryer; dictionary; encyclopedia; daily newspaper; three or more magazine subscriptions; black and white TV; color TV; car; second car; two bathrooms; tape recorder; home movie projector; home slide projector; typewriter; piano; and skis or golf clubs.

The organizations represented here today consider these questions on the family situation to be clear invasions of privacy of the student and of the home by the school system. Whatever the purpose of the Johns Hopkins University questionnaire, we strongly protest against this type of probing into the personal affairs of the student and his family life.

Let us turn next to the category of self-evaluation in the Johns Hopkins questionnaire:

Here, the student is asked whether he pretends to be busy in class when he is really just wasting time.

Whether being popular with other people his age is more important than anything else to him.

If someone often has to tell him what to do.

If he admires students who are very bright.

When he doesn't know the answer, if he will try to fake it rather than say he doesn't know.

Whether he will usually give in because he doesn't want to upset his friends.

If he knew the teacher was not going to collect his homework, whether he would do his best.

Whether he gets blamed for things that are not really his fault.

The student is asked if the best way to get ahead in life is to be nice to all people.

Whether he likes to be by himself because he has a lot of things he likes to do alone.

Whether he feels uncomfortable if he disagrees with what his friends think.

If the student sometimes feels angry when he doesn't get his way.

If it would be hard for him to face the "cold, cruel world."

If he can say "No" when his friends call him to do something with them.

He is asked whether he will put off leaving his home and friends for as long as possible.

If he didn't like the way things were going in a group, whether he would hesitate to tell the leader.

Whether he really cares if some people don't want to be friends with him.

Whether he tries to get out of doing work and hopes no one will find out.

If he prefers to let other people in a group make the decisions.

It is our view that this line of self-evaluation, self-analysis, self-criticism, and confession is pure and simple an invasion of psychological privacy of the child. Students of all ages are asked to direct their thoughts to introspection and unwittingly lay bare their inner-most feelings to the data collector for whatever purpose he may wish to make use of them.

Our third and final category of the Johns Hopkins test deals with feelings and attitudes toward the school and teachers:

The student is asked if he feels lost in school.

If he feels the tension build up in him when he is in school.

If he often does not know what he is supposed to do.

Whether most of his teachers want him to do things their way and not his own way.

Whether his teachers tolerate a lot of questions during a lesson.

If certain students in his classes are favored by the teachers more than the rest.

If the teachers in his school often act as if they are always right and he is wrong.

Whether he is considered weird when he gets involved and excited in his class work.

If he daydreams a lot in class.

Whether he wants to go to school.

Whether he ever does anything exciting in class.

If he counts the minutes until the class ends.

Whether he sits on the floor in many of his classes.

Whether most other students want to go to school.

If a diploma from his school means more that you behaved yourself than that you really learned something.

He is asked if he and his teachers are: (1) on the same wave length, (2) on the same planet, (3) somewhere in the same solar system, or (4) in two different worlds.

If his classwork is: (1) great stuff, (2) good stuff, (3) OK, or (4) dull stuff.

How he would rate the ability of most of his teachers compared to teachers in other schools at his grade level: (1) far above average, (2) above average, (3) average, (4) below average, or (5) far below average.

If he and the school are: (1) good friends, (2) friends, (3) distant relatives, (4) strangers, or (5) enemies.

The student is asked to provide the full names of his three best friends.

And also the full names of students in the following categories:

Very popular with other students;

Independent;

Hard to fool; and

Fools around in class instead of working.

The student is queried as to whether he was ever scolded in class for:

Fooling around;

Not paying attention;

Fighting in class;
Talking back to teachers;
Not handing enough work;
Telling off a teacher; and
Shouting or laughing out loud.

If he ever stayed away from school just because he didn't want to go: (1) never, (2) 1 or 2 days, (3) 3 to 5 days, or (4) more than 5 days.

Whether he has ever cut classes just because he didn't want to go to them: (1) never, (2) 1 or 2 classes, (3) 3 to 5 classes, or (4) more than 5 classes.

A lot of the questions in the Johns Hopkins survey relating to student feelings and attitudes toward school and teachers are simply absurd and a sheer waste of time and resources. Perhaps the most ridiculous question is the one asking students to rate teachers in other schools at the same grade level. Leaving aside the ability of a young student to evaluate his teachers, how could he be expected to compare them with teachers in other schools whom he has neither seen nor heard? A good many of the queries are negative in tone; in our judgment they foment inner frustrations in the students and create student animosity toward the teachers and the particular school attended. As I have indicated, the regular classroom teacher is not involved in this test and is therefore unable to respond or even know about the criticisms by the students. But the most damaging questions in this category are those which extract self-incriminating information from the students themselves on truancy, insolence, and other improper activities in school. Self-confessions by students on such things as fighting in class and telling off the teacher provide an evaluation team with data to be entered into a permanent personality record classifying students as maladaptive, agressive, antisocial, emotionally disturbed, and predelinquent.

The Johns Hopkins test may have run its course for this year with the students, but the survey continues for teachers and parents. We are asking that this project be withdrawn forthwith and prevented from spreading to other counties in the State of Maryland.

Our second candidate for removal from Maryland public schools is a questionnaire currently being administered to 50 classes in 26 elementary schools in Montgomery County. This survey, which is being financed by the Spencer Foundation, is designed to gain insight into students' motives and goals and likes and dislikes. In addition, assessment of the children's educational growth, with both standard academic measures and some non-academic measures, will be made toward the end of the school year. According to an explanatory letter to parents by a psychologist with the Psychological Services Department of the Montgomery County Public Schools system, "characteristics of the classroom environment will be assessed by observers in a series of several visits during the year." The information gained by this project will be sent out of State and fed into computer data banks for use in diagnosing and prescribing the handling of students.

Some sample questions from the Spencer Foundation survey are:

If your parents tell you you're acting silly and not thinking clearly, it is more likely to be: (a) because of something you did or (b) because they happen to be feeling cranky?

Suppose your parents say you aren't doing well in your school work. Is this likely to happen to you: (a) because your work isn't very good or (b) because they are feeling cranky?

If your parents tell you that you are bright and clever, is it more likely: (a) because they are feeling good or (b) because of something you did?

The students are asked to answer a number of I think I am questions, circling the appropriate degree to which they are:

Able to get along with other kids;
Not able to figure things out in school;
Scared to take chances;
A good worker in school;
Happy with myself;
Not as smart as other kids in school;
Trying my best in school;
Not the way I would like to be;
Sure of myself;
Doing poorly in school; and
Angry with myself.

The complaints and concerns of the organizations represented here today are by no means limited to specific surveys, such as those financed by the National

Institute of Education and the Spencer Foundation. We are opposed to all abuses by the schools of the right to privacy, the right to be left alone. It so happens that the school administrative personnel and the social researchers in the State of Maryland have found a veritable gold mine in grants, contracts, and techniques that are turning public school children into a collection of guinea pigs who are constantly being battered with questionnaires, personality tests and a variety of other inquisitions which are clearly invasions of privacy of both the student and the home.

To cite one widespread example, the Maryland State Board of Education By-laws call for a compulsory treatment of subject matter known as Interpersonal Relationships. No child in public schools in the State of Maryland may be excused from these discussions and classroom activities, which are interspersed throughout the curriculum from kindergarten through the 12th grade. Under this program, children must be subjected to all types of probes into their psyches and family situations. Here in Montgomery County, for example, elementary school children are forced to participate in the following material and questions:

Discuss family size, pointing out advantages of both large and small families.

Role play the family at dinner.

Role play an increase in conflicts with parents.

Role play other meaningful family situations.

Have children keep records of their activities; note those children who seem to be overburdened with responsibilities.

Have children write paragraph about being afraid; encourage them to verbalize their fears due to dark places, being hurt, dreams or nightmares, personal loss, experience with death, punishment, and the unknown.

Have children observe their family for a week; have them jot down notes on the way love was shown.

Have children write examples of times when they felt angry, afraid, shy.

Have role playing situations based on these experiences.

Here are some sample questions:

What kind of things make you angry?

What do you like to do when you are alone?

Should you expect to be paid for chores done at home?

Whom does your family entertain at your house?

How do you cooperate with your family?

What happens when and if you refuse to cooperate?

Do you think you are being treated fairly?

Do you think you would like to live and work alone?

What do you expect of your father and mother?

Under what circumstances have you felt unloved, unwanted, lonely, shy, or fearful?

As these examples from the K-through-6 curriculum demonstrate, the Interpersonal Relationships approach emphasizes negative attitudes; it dwells on fears, death, sorrows, anxieties, and other personal feelings and the interrelationship of these factors with parents and the home situation. The student—particularly the younger child—has a weak defense against such techniques and can easily be induced to yield to classroom pressure or forced to work his imagination overtime for the sake of satisfying the teacher's demands.

Such prying by the schools into the home and into parental authority can be a most dangerous business. In Montgomery County, the School Board recently (August 27, 1973) approved an expanded definition of child abuse, under which teachers are asked to make official reports to the police and the social services authorities on children who have been "denied normal experiences that produce feelings of being loved, wanted, and secure." These are labelled as children who have been subjected to so-called "emotional neglect." Moreover, teachers are required to submit a report on any child who is "overworked" by his parents or exposed to "continuous friction in the home." Whatever the charge, the school system policy stipulates "if there is any doubt or question in reporting such cases, it should be resolved in favor of the child."

It can, of course, readily be appreciated by one and all that the questions in the compulsory Interpersonal Relationships curriculum as well as a good many of the questions in the Johns Hopkins survey could provide data which may well be diagnosed incorrectly or misinterpreted by the social scientists as child abuse or child neglect cases. Moreover, many children could be labelled as what the social engineers like to call "disadvantaged children." We parents are most disturbed over this kind of role being assumed by the public schools. The schools

were established in the United States to provide a service to the parents and taxpayers. The schools, therefore, work for us; not the other way around. The teachers, who in our view are thrust into and trapped in the middle of the situation, have an equally valid and justifiable complaint.

Whatever the stated goal of the educators and the social planners, the whole question of labelling children and predicting their behavior on the basis of questionnaires and classroom confessions is being challenged by parents and legal authorities throughout the United States. An important question is: Who has access to the data? Another, how will the data be used? An even more important question might be: What are the values and attitudes of the evaluators? The Congress of the United States is very much concerned with all of these questions. And we here today, who speak for five citizens organizations with representation from eight Maryland counties, feel that the Maryland State public officials should be similarly concerned.

Therefore, by letter of April 19, 1974, we are strongly urging the Governor of Maryland to take steps to remove the Johns Hopkins University survey, the Spencer Foundation survey, and all similar tests and activities from the public schools of Maryland and to charge the Maryland State Board of Education with the task of reviewing all curriculum and practices in the classrooms for the purpose of removing those parts which violate the rights of the students and the parents as guaranteed by the Constitution of the United States of America. We are saying to the Governor "Enough is enough." We are asking him to remove the inquisitions of the master social planners from our public schools and to ensure us that our educators will concentrate, instead, on the basic concepts of education which our tax dollars were intended to finance, and education that will assist and prepare our children to face a mature, real world.

Mr. BIDEN. Mr. President, is the parliamentary situation such that I still have a few minutes of the time yielded to me by the Senator from New York?

The PRESIDING OFFICER. The Senator was yielded 5 minutes. One and a half minutes of that time still remain.

Mr. BUCKLEY. Mr. President, I yield 2½ minutes to the Senator.

Mr. BIDEN. I have one question. In subsection (b)(2), does the Senator have any objection to removing the words "or principal effect" on line 19, page 3, where it reads "the primary purpose or principal effect of which * * *"?

Mr. BUCKLEY. No, I do not. I think that would be very helpful. I thank the Senator from Delaware for suggesting it.

Mr. President, I ask unanimous consent that the three words at the end of line 19 on page 3 be eliminated.

The PRESIDING OFFICER. Is there objection? Without objection, the amendment is so modified.

Mr. BIDEN. I have no further questions of the Senator. He has indicated to me, in private and in the colloquy, that this is intended to go only to those programs which would be considered experimental. I think the single most burning issue before the country is the invasion of privacy at all levels. School records are private. No one should have access to them unless it is with the consent of the parents.

I am glad to be a cosponsor of the amendment.

Mr. HART. Mr. President, would the Senator yield for 1 minute?

The PRESIDING OFFICER. Who yields time to the Senator from Michigan?

Mr. PELL. I yield 1 minute. Which side is he on?

Mr. HART. I guess my honest answer is that I do not know which side I am on. I wish we had had a study or report on it. To say that the programs for research and experimentation are to be prevented unless the parents say OK is something unique and not really in the nature and order of the evolving educational techniques, when, on page 4 it is stated:

As used in this subsection, the term "research or experimentation project" means any project or program which is a part of an applicable program and which is authorized by an administrative officer of an education agency, a State or local education agency, or any education institution, including preschools, except that research or experimentation projects shall not include projects in the field of reading . . .

Maybe that is visual education. I do not know.

It seems to me that the definitions excludes experimentation on anything except speech and language. However, this is but one example of the difficulty I have and that other Senators have in considering and understanding the reach of the bill without hearings. Of course, everyone is for protecting privacy; that is great. However, what do we do with experimentation?

Mr. BUCKLEY. Mr. President, I should like to address myself to the remarks just made. First of all, the amendment explicitly excludes reading and bilingual education. However, some parents might choose to have their child take those subjects. They do not destroy the educational apparatus of this program. They do not destroy the ability to develop a program with cooperative parents. If a program is so alarming to the average parent that no parent will cooperate, then we should examine the program to see whether that program should be in effect. I do not believe that the remarks dealing with such affairs would be justified.

Mr. HART. Mr. President, what about the new math, which I still do not understand, but to which my children have been exposed? Could I say "no" if we were to adopt this amendment?

Mr. BUCKLEY. That is not at all the situation. A normal person would agree to experimentation with new math.

We are not talking about educational disciplines or perhaps new textbooks or new apparatus, or anything else along that line. We are talking about new departures from teaching methodology.

Mr. MATHIAS. Mr. President, if the Senator would yield me a minute to pursue that line of inquiry, as much as I want to share that concept, I share with the Senator from Michigan some lack of comprehension as to whether it will do this. The Senator from Michigan raises a question about new math or any other method of teaching a new subject. What about the question I asked earlier as to whether this amendment would prevent any identification symbol? If students cannot be identified in a statistical sense, how can we make any kind of longitudinal studies as to whether a new teaching program on any subject is successful? How do we evaluate programs? How do we make any judgments beyond the isolated case of one student at a time?

Mr. BUCKLEY. Mr. President, schools are quite capable of evaluating the experience with students which they have in their own classes. I see no difficulty at all. Again, I think the Senator is emphasizing that the amendment is not restroying the ability of programs or research to go forward in the case of experimental programs.

All the amendment requires is no identification, and then the parent has the right to withdraw the child. He does not need to consent in advance. In general, the premise is that parents are generally responsible adults, having prime responsibility for their children. I have no doubt that they would act responsibility.

The PRESIDING OFFICER. Who yields time?

Mr. PELL. Mr. President, I yield myself 5 minutes.

I think the junior Senator from New York knows of the regard and high respect I hold for him. As much as I would like to see the Senator succeed in his proposal as he explains it, we are concerned here not with what the Senator from New York intends the language he proposes to accomplish. It is what the language would do.

This is what bureaucrats in future years will rely on, what the language in the bill is.

They will not look up the debate on the floor at the time of passage of the bill. However, the language of the bill reads specifically:

"Parents should be informed in advance and in writing of the participation of their child in any research program which is part of a school program * * * parents of such child objects to participation."

I believe that this language says that it there is to be a new experimental program of learning new math, or a psychological program, or something of that sort, every parent must be informed in writing. We should consider the postage and redtape involved. It would kill most new programs.

I hope the Senator from New York might be willing to withdraw at least subsection (b). I wonder what the wishes of the Senator might be in that regard.

Mr. BUCKLEY. Mr. President, a parliamentary inquiry.

The PRESIDING OFFICER. The Senator will state it.

Mr. BUCKLEY. Mr. President, is it not possible to have a division ordered so that we could vote on section (b) alone?

The PRESIDING OFFICER. If it is in the pending provision, the answer is yes.

Mr. BUCKLEY. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. On whose time?

Mr. DOMINICK. Mr. President, will the Senator withhold that request for just a moment?

Mr. BUCKLEY. Mr. President, I withhold my suggestion of the absence of a quorum.

Mr. DOMINICK. Mr. President, I want to ask the Senator, not about section (b), because I must say that I share my compatriot's concern over that. But on section (c) I have been very active since I became a member of the Education Subcommittee in trying to make the program available for children who are going from high school to college or graduate school.

It looks to me as though what we have done under subsection (c) is to prevent whatever institution might be seeking the records of a youngster concerning his personality to determine whether he is eligible (a) either for a loan, or (b) for a work-study program, or (c) for a well deserved and perhaps not fully qualified minority student, as to his ability to get this background without the consent of the child's parents. He may be trying to get away from the parents, who may be lushes, and he may be trained to get away from them.

Mr. BUCKLEY. I would point out that the amendment states that—

"Whenever a student has attained eighteen years of age, the permission or consent required of the student shall thereafter only be required of and accorded to the student."

Mr. DOMINICK. Mr. President, I understand that. However, I would presume that the Senator from New York or any Senator, as well as the Senator from Colorado, went to college when he was 17. A great number of children go to college when they are 17.

All I can say is that I think this is just a roadblock. It is something which I do not think the Senator from New York wants to do, in which we are trying to promote this subject and are not trying to restrict it.

I think that what the Senator is driving at in section (c) is the relief of a group of people who are trying to make some kind of psychiatric research program, totally devoid of the educational process in order to get their master's thesis or write something for the Brookings Institution, or something of that kind.

I am afraid that the language goes much further than that kind of restriction.

Mr. BUCKLEY. I find it implausible that parents would not cooperate in helping a child qualify for financial help.

Mr. DOMINICK. Well, they would not hesitate if he were going to be bringing the financial help back home, but I know a great number of people who do not give a whoop whether their children go to college, graduate school, or anything else; in fact, they would prefer they did not, and if he is trying to get a loan all of a sudden which they may ultimately be called on to repay, they may say no.

Mr. BUCKLEY. I point out to the Senator from Colorado that on page 6, line 12, we make an exception for financial aid.

Mr. DOMINICK. That is true. I had not seen that. Does that apply to all of subsection (c)?

Mr. BUCKLEY. Yes, it does.

Mr. DOMINICK. That helps materially. I will go back to the drawing board.

Mr. BUCKLEY. I thank the Senator.

Mr. President, in an attempt to make this amendment as acceptable as possible, I would make at this time, in response to some of the concerns expressed by the Senator from Maryland and the Senator from Michigan, the following modification: On page 4, line 13, to add in, as an exception in the definition of experimental programs, after the words "bilingual education", the words "or for the development of new techniques for the teaching of traditional disciplines". I ask unanimous consent that I may so modify my amendment.

The PRESIDING OFFICER. Without objection, the amendment will be so modified.

Mr. PELL. Mr. President, reserving the right to object, I could not hear. What was the modification?

Mr. BUCKLEY. On page 4, line 13, after the word "education," I insert the words "or for the developing of new techniques for the teaching of traditional disciplines."

The PRESIDING OFFICER. Without objection, the amendment is so modified.

Mr. PELL. Mr. President, I will not object to the modification, but this will be the fourth modification made on the floor. I realy think this matter should be considered in the committee. I shall be compelled to vote against it, but I do not object to the modification.

Mr. BUCKLEY. May I now ask the Presiding Officer whether the Parliamentarian has made a determination as to whether section (b) would stand on its own?

The PRESIDING OFFICER. (Mr. TUNNEY). Section (b) is written in such a way that it is independent and is divisible.

Mr. BUCKLEY. Under those circumstances, Mr. President, and on condition that the sponsor will accept the balance of the sections—Mr. President, if I may have the attention of the distinguished manager of the bill—I am willing to ask for a division, so that we may vote separately on section (b), provided the manager will accept the remainder of the amendment.

Mr. PELL. I would ask for a rollcall vote on subsection (b), and as far as section (c) goes, I would ask my colleague from Alaska whether he has any objection.

Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. On whose time?

Mr. PELL. To be equally divided.

The PRESIDING OFFICER. Without objection, it is so ordered. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

Mr. PELL. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. PELL. This procedure would be acceptable, and I am perfectly willing to have either a voice or a division vote on sections (a), (c), and (d).

Mr. BUCKLEY. Mr. President, before asking for a division, I ask unanimous consent to have printed in the RECORD a statement prepared by the Senator from Arizona (Mr. GOLDWATER) in support of this amendment.

The PRESIDING OFFICER. Without objection, it is so ordered.

STATEMENT BY SENATOR GOLDWATER

PARENTAL AND STUDENT RIGHTS

Mr. President, it gives me great pleasure to join with my good friend from New York, Senator Buckley, and others of my colleagues, in sponsoring an amendment to protect the right of privacy of school children and their parents. I have a particular interest in the amendment because it would legislate in the education field certain, basic safeguards for the right of personal privacy which I have been trying to get enacted for over a decade.

Subsection (a) of our amendment would provide statutory confirmation of the right of parents to see the contents of their own children's school records. Parents would also be guaranteed a right to challenge information in their child's school records and to correct any inaccurate or misleading data. This is identical to the safeguards standards which are included in S. 2810, a bill which I have introduced regarding the privacy and accuracy of personal data systems of all types.

Subsection (b) of our amendment would create a system of parental consent which would give parents a right of control over "personality" tests given to their children in the public schools. This provision is identical to legislation which I first introduced thirteen years ago, in 1961. In the early '60's, I was concerned that the new Federal authorities for direct funding of educational programs, which were just getting underway, would allow Federal monies to be spent for testing programs in which school children could be used as involuntary "guinea pigs" in experimental programs unrelated to the true purposes of education.

Needless to say, Mr. President, I was shocked to learn of the existence of surveys being conducted in our public schools which probed the most intimate personal aspects of the lives of school children and their relationships with their parents and families. I was especially surprised to discover one survey, financed with Federal funds, which consisted of some two hundred questions being asked of Junior High School students ranging in age from 11 to 14 years.

These questions inquired of the student:

"Is your father fairer about punishment than your mother?"

Did you "steal more than $2 from your parents?"

Did you "fight physically and bodily with an adult relative?"

The student was also asked to reveal to the school whether he or she had "gone further than petting with a person of the opposite sex."

In addition, the student was asked to rate his or her own family. The student was required to give a yes or no answer, for example, to these questions:

"I wish my family had nearly as much money as the families of many of my classmates."

"Are the children in your family punished more severely than in other families?"

"I wish my father and mother were better educated, like the parents of many of my classmates."

Mr. President, these questions were just a few of the two hundred questions that were actually being asked of American school children in a questionnaire financed in part by Federal funds granted by the Department of HEW.

Yet, I was told it wasn't done. I was told it couldn't be done. On the one hand, I was informed that such questions were not permitted under the administrative interpretation of the Department. On the other, I was advised that leading "experts" believed that my amendment "would greatly inhibit much-needed educational research. . . ."

So there you have it, Mr. President. The agency told me that my amendment was not needed because it would duplicate their own policy interpretations; but that if it was put into law, it would impair research that the bureaucrats wanted to allow to go on. I never could make sense out of this, but the Department's view prevailed and the Senate rejected my amendment.

Mr. President, perhaps the climate of this country has caught up with the wishes of ordinary parents and ordinary school children. Perhaps the concept of the personal freedom of the average citizen and his family has grown to the point where Congress is willing to be the guardian of his privacy against prying and inquisitive minions of the bureaucracy.

Mr. President, our public schools have no compelling need for psychological and personality tests which pry into the private lives of a captive audience of school children. Even if the child is not specifically told that he is required to answer these tests, it would be a rare and unusual child who would dare to defy the authority of a school by refusing on his or her own initiative.

Questins of this kind are an intolerable invasion of the right of privacy. They exemplify the ever-watchful eye of "Big Brother" spying into the most personal thoughts and habits of American families, and doing it, by abusing the trust of innocent school children.

Moreover, Mr. President, these types of questions are calculated to raise doubts, suspicions, and hostility in the minds of our children toward their own parents and a skepticism about the basic moral principles of our society. In this sense, these tests could be used by governmental planners for purposes of influencing or conditioning the social and political thinking of our youth, and through them, American society.

Mr. President, the time to preserve what is left of our personal privacy is now. Sufficient thought and action must be given to the problem while there is still some measure of personal liberty left to cherish. It is for us today to determine just how much freedom shall remain for the individual in the future. I implore my colleagues to vote for the Parental and Student Rights Amendment.

Mr. President, I include the junior high school student survey which was conducted in the early 1960's, in part with Federal grants:

JUNIOR HIGH SCHOOL SURVEY SUPPORTED BY GRANTS FROM THE U.S. PUBLIC HEALTH SERVICE AND THE UNIVERSITY OF KANSAS (1961)

FACTS ABOUT YOURSELF

Please answer all questions completely.

5. How old are you? (Check only the answer.)
(1) —11 years or younger.
(2) —12 years old.
(3) —13 years old.
(4) —14 years old.
(5) —15 years old.
(6) —16 years old or older.

6. Sex:
(1) —Boy.
(2) —Girl.

7. What grade in school are you now in?
(7) —Seventh grade.
(8) —Eighth grade.
(9) —Ninth grade.

8. Are you (check only one answer) —
(1) —An only child?
(2) —The youngest child in your family?
(3) —The oldest child in your family?
(4) —Neither the youngest nor the oldest child?
9. How many living brothers and sisters do you have?
(0) —None.
(1) —One.
(2) —Two.
(3) —Three.
(4) —Four.
(5) —Five or more.
10. What was the highest grade your father finished in school?
(1) —Eighth grade or less.
(2) —Some high school.
(3) —Finished high school.

PART I. RULES WE ALL BREAK

The questions in part I are about more personal things concerning you and your friends. Do you put your name or address on this questionnaire. We want to assure *you* that your answers will be kept completely *secret* and *confidential*. No one will ever know how you answered any of the following questions. We encourage you to be completely honest with your answers.

For the purpose of this study, we are interested in the things you have done during the *last 2 years only*.

11. Damage or disfigure furniture in schools, such as chairs, tables, and desks:
(1) — No.
(2) — Yes.
12. Steal goods from warehouses or storagehouses:
(1) — No.
(2) — Yes.
13. Damage cemetery property;
(2) — Yes.
(1) — No.
14. Damage or destroy public signs or roads markers:
(1) — No.
(2) — Yes.
15. Steal automobile parts such as hubcaps, mirrors, ornaments, etc.
(1) — No.
(2) — Yes.
16. Kicked, bit or scratched a student of about your own age:
(3) — Three or more times.
(2) — Twice.
(1) — Once.
(0) — Never.
17. Get out of going to school by writing a fake excuse for yourself:
(2) — Yes.
(1) — No.
18. Steal or siphon gasoline from cars, trucks, or other kinds of vehicle equipment;
(2) — Yes.
(1) — No.
19. Damage or destroy mailboxes:
(1) — No.
(2) — Yes.
20. Steal more than $2 (money) from your parents:
(2) — Yes.
(1) — No.
21. Puncture or cut automobile tires, bike tires:
(1) — No.
(2) — Yes.
22. Steal materials or equipment from buildings that are being constructed:
(2) — Yes.
(1) — No.

23. Kicked, scratched or bit an adult relative (mother, father, guardian, or uncle, for example) :
(0) — Never.
(1) — Once.
(2) — Twice.
(3) — Three or more times.
24. Damage or destroy toys or games that belonged to persons your own age:
(1) — No.
(2) — Yes.
25. Steal from buildings that are being torn down :
(1) — No.
(2) — Yes.
26. Tied a person up with rope, string, or wire to a tree or similar object and then left them that way :
(0) — Never.
(1) — Alone.
(2) — With one or more others.
(3) — Both alone and with others.
27. Steal things from your parents that were worth more than $2 :
(2) — Yes.
(1) — No.
28. Teased severely, hurt or killed a cat or dog :
(1)—Alone.
(2)—With one or more others.
(0)—Never.
(3)—Both alone and with others.
29. Scratch the paint on someone's car on purpose :
(1)—No.
(2)—Yes.
30. Steal more than $2 (money) from your brothers or sisters :
(2)—Yes.
(1)—No.
31. Skip school with one or more friends or classmates :
(2)—Yes.
(1)—No.
32. Steal articles of clothing worth more than $5 from clothing or department stores :
(1)—No.
(2)—Yes.
33. Become so mad or angry that you threw things at or hit a teacher or principal or other school official :
(3) Both alone and with others.
(0)—Never.
(1)—Alone.
(2)—With one or more others.
34. Steal a bicycle from anyplace other than a place that sells bicycles (like from neighborhoods, school grounds, or public places where bikes may be parked) :
(2)—Yes.
(1)—No.
35. Remove spark plugs or wires from cars :
(1)—No.
(2)—Yes.
36. Steal a car for joyride without the owner's knowledge or permission :
(2)—Yes.
(1)—No.
37. Break or crack windows in automobiles :
(1)—No.
(2)—Yes.
38. Skip school with three or more friends or classmates :
(2)—Yes.
(1)—No.
39. Steal articles of clothing worth less than $5 from clothing store or department store :
(1)—No.
(2)—Yes.

40. Damage flowerbeds or gardens on purpose:
(2)—Yes.
(1)—No.
41. Steal gasoline from gas stations, farms, or other private places:
(1)—No.
(2)—Yes.
42. Taken part in fights where knives or switchblades were used:
(1)—No.
(2)—Yes.
43. Steal a bicycle from a store that sells or repairs bikes:
(2)—Yes.
(1)—No.
44. Skip out of certain class periods, but not the whole day, without permission (like gym class or student assemblies):
(2)—Yes.
(1)—No.
45. Fought physically and bodily with an adult relative such as mother, father or aunt (that is, fought in anger or fear, not in sheer fun):
(0)—Never.
(1)—Alone.
(3)—Both alone and with others.
(2)—With one or more others.
46. Steal things (not money) from your brothers or sisters that were worth more than $2:
(2)—Yes.
(1)—No.
47. Get out of school early by pretending to your teacher that you were sick or not feeling well:
(2)—Yes.
(1)—No.
48. Steal anything because an adult asked you to steal it:
(1)—No.
(2)—Yes.
49. Beat up a person much older than yourself in a fight:
(0)—Never.
(2)—With one or more others.
(1)—Alone.
(3)—Both alone and with others.
50. Steal more than $2 (money) from your friends or classmates:
(2)—Yes.
(1)—No.
51. Damage parking meters on purpose (break glass, jam slot):
(1)—No.
(2)—Yes.
52. Steal jewelry worth more than $2 from jewelry, department, dime or drug stores:
(2)—Yes.
(1)—No.
53. Skipped school or stayed out of school without a genuine excuse for more than 1 day:
(1)—No.
(2)—Yes.
54. Damage or break coin machines of any kind on purpose:
(1)—No.
(2)—Yes.
55. Damage or ruin personal clothing of classmates or other schoolchildren:
(1)—No.
(2)—Yes.
56. Get out of going to school by pretending to your parents that you were sick:
(2)—Yes.
(1)—No.
57. Steal more than $2 (money) from candy, coke, or cigarette machines:
(2)—Yes.
(1)—No.
58. Leave home with intention of going to school, but just never making it to school (without a good reason):

(1)—No.
(2)—Yes.
59. Injured or hurt someone not in your family, but arranged matters so that someone else got the blame:
(1)—Alone.
(2)—With one or more others.
(3)—Both alone and with others.
(0)—Never.
60. Steal more than $52 from school:
(2)—Yes.
(1)—No.
61. Leave school early without permission:
(2)—Yes.
(1)—No.
62. Try to "get by" without paying the bill in restaurants, cafes, soda fountains:
(1)—No.
(2)—Yes.
63. Skip school by yourself without good excuse from parents:
(2)—Yes.
(1)—No.
64. Taken part in a gang fight against another gang or against one or two other persons:
(1)—Once.
(2)—Twice.
(3)—Three or more times.
(0)—Never.
65. Steal things from inside of parked cars:
(1)—No.
(2)—Yes.
66. Break windows on purpose in vacant homes, garages, or other buildings:
(1)—No.
(2)—Yes.
67. Damage or destroy anything because someone "dared" you to do it:
(1)—No.
(2)—Yes.
68. Steal things worth more than $2 from foodstores:
(2)—Yes.
(1)—No.
69. Damage school property other than chairs, tables, and desks:
(1)—No.
(2)—Yes.
70. Curse or use obscene language in speaking to a teacher or other school official:
(2)—Yes.
(1)—No.
71. Steal anything and then sell it to an older teenager or adult:
(1)—No.
(2)—Yes.
72. Damage or destroy anthing that belonged to another person, in order to "get even" with that person:
(1)—No.
(2)—Yes.
73. Steal money from public telephones or parking meters:
(1)—No.
(2)—Yes.
74. Hit or strike a teacher, coach, or other school official:
(2)—Yes.
(1)—No.
75. Take part in fights where BB guns, airpellet guns, or slingshots were used:
(1)—No.
(2)—Yes.
76. Tease or embarrass someone by stripping or taking his or her clothes off?
(2)—Yes.
(1)—No.
77. Damage or destroy anything "just for the heck of it":
(1)—No.

(2)—Yes.
78. Steal less than $2 (money) from candy, coke, or cigarette machines:
(2)—Yes.
(1)—No.

PART II. ALONE OR WITH OTHERS

Instructions.—We are interested in how certain rules are broken. Some people break rules only when they are with others, some break rules only when they are alone, and other persons. For each item, *check the box that applies to you.* If it does not apply to you, leave that item blank.

In the last 2 years, did you:

	Only when alone (1)	Only when with other persons (2)	Both alone and with other persons (3)
11. Steal hubcaps, mirrors, etc. from cars			
12. Puncture or cut tires, convertible tops, scratch the paint on cars			
13. Tie a person up with rope or string and left them that way			
14. Tease, hurt, kill harmless animals			
15. Steal lothing worth less than $5			
16. Steal a car for a joyride			
17. Beat up a person much older than you			
18. Damage or break coin machines			
19. "Get by" without paying the bill in cafes, soda hops, movies, other events			
20. Damage school property on purpose			
21. Steal things in order to sell them			
22. Damage or destroy road markers, signs, mailboxes, street lights			
23. Steal anything worth more than $5 but less than $50			
24. Beat up an adult for his money			
25. Steal anything worth $50 or more			
26. Break into and enter a locked store, gas station, or other buildings			

PART III. YOUR SOCIAL ACTIVITIES

Instructions.—In this section are statements about what some boys and girls do most of the time in their time after school and on weekends. Read each statement and decide whether it fits you or does not fit you as you are right now or during this year. If the statement is true of you, that is, if you would say "*Yes*" to the statement, put a No. 1 next to it. If the statement is not true of you, that is, if you would say "*No*" to the statement, put a No. 2 next to it.

Be sure to read and to answer each statement with a 1 or a 2. If it fits you fairly well but not exactly, put a 1.

Answers.—Put 1 for a "*Yes.*" Put 2 for a "*No.*"

27. I spend a lot of time with one special friend who is not a member of my family.—
28. I stick pretty much to myself.—
29. I never disobey my parents.—
30. I spend a lot of time with one friend at a time, although I have several close friends.—
31. I spend a lot of time with two or three friends. The group of us play together.—
32. I do some talking about or listening to talk about sexual matters when I am with my friends.—
33. I play with a large group of four or more children in or near my home neighborhood.—
34. I mostly play alone or with my brothers or sisters.—
35. I belong to a group that is often chased after by some adults such as storekeepers, police, or homeowners.—
36. I never catch cold in the winter or spring.—
37. I play with friends my parents do not like.—
38. I never tell lies.—
39. I often share secrets and ideas or hopes with my friends.—
40. I have taken part in kissing and necking while on a date or while alone with a person of the opposite sex.—
41. Most of my friends are my own age or between 11 and 14.—
42. I have never spent a night in a detention home or jail.—
43. Most of my friends are 2 or 3 years older than I am.—

44. I have petted with a person of the opposite sex while on dates or when we were alone.—
45. Most other boys and girls like me.—
46. I try to get other boys and girls to like me.—
47. I have gone further than petting with a person of the opposite sex.—
48. I care a great deal about what other boys (or girls) think of me.—
49. I want to be different somehow from others in my own age group.—
50. I have answered ads in comic books or other magazines which advertised pictures, photographs, or stories about sexual matters.—
51. I like most of all to spend my free time alone.—
52. Some of my friends do not like the way I act.—

PART IV. LEISURE ACTIVITY AND FAMILY LIFE

Instructions.—The statements in this section are like those in the section you just completed. But these have to do with *how* you spend your spare time and how you are treated by your parents.

Read each statement. If it applies to you as you are right now or have been during this year, mark the statement with a 1 for a "*Yes.*" If it does not apply to you, mark it with a 2 for a "*No.*"

The statements.—Write 1 for a *Yes*, and 2 for a *No.*

53. Do you spend more of your free time with your friends than with your family?—
54. Do you go to dances more than once a month?—
55. Do you go out with your mother or father more than once a month? (Movies, dining, social events, etc.)—
56. Is your father fairer about punishment than your mother?—
57. Do you study schoolwork at home less than five times a week?—
58. Is your mother fairer about punishment than your father?—
59. Do you work at a part-time job once or more a week?—
60. When you do something extra, do your parents reward you with praise or special privileges or with money?—
61. Do you help around the house doing chores almost every day?—
62. When you have done something wrong or "bad" do your parents try to reason with you?—
63. Do you usually attend at least one movie a week?—
64. Are some children in your family punished more severely than others?—
65. Do you spend time after supper at a local hangout (drugstore, soda shop, bowling alley, etc.) at least two times a month?—
66. Do your parents get all the facts before they punish you?—
67. Do you usually have one or two dates a month or more?—
68. Are the children in your family punished more severely than in other families?—
69. Do you think that your friends have better ideas than your parents do about what a young person should do in his spare time?—
70. Do you usually spend three or more evenings a week away from home?—
71. Are the children in your family ever punished when they do not need it?—
72. Does your father punish you when your mother does not think you should be punished?—
73. Would you like to spend more of your free time with your friends than your parents now allow?—
74. Does your mother punish you when your father does not think you should be punished?—
75. Do you feel your mother punishes you fairly?—
76. Do you feel your father punishes you fairly?—
77. Below is a line that stands for your *grades* or *marks* in school this year, thinking of them lumped together. Make only one check (√) where you best fit.

"A" or best possible, 100.
"B" or high, 90.
"C" or average, 80.
"D" or below average, 70.
"F" or failing, 60.

PART V. GUESSING CAUSES

Instructions.—Reprinted below is a news story that appeared not long ago in the Kansas City Star. After you read the story carefully, pretend that you are talking the story over with some school friends. None of you knew the boy in

the story directly or indirectly, but you are all *guessing* about why he did what the police claim he did. Then the questions that follow the story, indicating what your guesses would probably be. (Names and places in the story have been added or changed.)

THE STORY

The Kansas City Police last night arrested Walter Stevens, age 13, who was caught by Police Sergeant Daniels. Daniels charged the boy with stealing coins from the coin machine and washing machines in the Whirlaway Laundromat. The policeman said he saw Stevens pry open the coin slots on the machines and remove quarters and dimes. He had $15 in coins in his pocket when arrested.

The boy's mother, Mrs. William Stevens, said she thought her son was at work at his part-time job in the nearby Roll Em Bowling Alley. He had worked there 2 nights a week for 2 months, she said, and had been earning about 60 cents an hour. The boy's father, William Stevens, 48, is a clerk in the central post office. He works the night shift and was away at the time of the arrest.

Walter Stevens is a seventh grade student at Wiltmore Junior High School. The Wiltmore principal, Mr. John Savage, reported that young Stevens had been doing very poorly in school for several months, and said that he had been expelled once for breaking school property and had often skipped school.

When interviewed, young Stevens told this reporter that his father had to work such long hours that he was very seldom home and that his mother was often ill and had to remain in bed. He claimed, "Nobody at school understands me or tries to help me."

Instructions.—Now check the statements below that you think provide the best possible explanations for why Walter Stevens did what he did. Remember that these are guesses and that all of them may be true or all may be false.

Put a 1 if you agree, and a 2 if you disagree.

11. Walter wanted to get more money than he could earn at his job in order to help his poor parents.—

12. Walter was lonely and unhappy at school, where no one understand him.

13. Walter was raised by bad standards and had not been taught properly what was right and wrong.—

14. Walter had everything against him. He was bound to get into trouble when everything at school and at home went wrong.—

15. Walter was fired from his job at the bowling alley but didn't want to worry his mother, who needed the money he had been giving her.—

16. A gang of young boys managed by a professional thief had organized stealing from laundromats and other service stores, and Walter had fallen in with this gang through his acquaintances at the bowling alley.—

17. Walter liked to steal and had probably been stealing one thing and another for several years before he was caught.—

18. Walter was sick, mentally or physically, but no one at school or at home understood this and helped him.—

19. Other children at school had been selfish and unkind in the past and had kept Walter from building any friendships. His loneliness led him to steal.—

20. Older boys in a gang really broke the coin machines and did the stealing, but they left Walter, who thought they were his friends, when they heard the police car and dumped the coins into his pocket.—

21. Walter's parents had never taken him to Sunday School, where he could have learned what is right and wrong.—

22. Walter wanted to find a way to get decent clothes and money for an allowance. His parents could not give him these things, but he needed them to try to make friends at school.—

PART VI. WISHES

Below are listed some wishes that have been expressed by boys and girls in other junior high schools. Read each wish carefully. Then check the wish with an X if you feel it is a wish that you have made or thought about any time during this year. If the wish does not fit you, leave it blank.

Check (X) here

23. I wish I could buy my lunch in the cafeteria more often.—

24. I wish I could afford to go the movies as often as many of the others in my school.—

25. I wish my family could take me on vacation trips like those that many of the persons in my school have enjoyed.—

26. I wish I were able to dress as well as most or many of the persons in my school.—
27. Many of the students in my class will get to go to college some day, but I probably won't get the chance.—
28. I wish I were physically better built or more attractive.—
29. I wish I were as attractive to the opposite sex as many of my schoolmates.—
30. I wish I could joint the Boy or Girl Scouts like many of my classmates.—
31. I wish my parents were more understanding, like the mothers and fathers of many of my classmates.—
32. I wish my family had nearly as much money as the families of many of my classmates.—
33. I might like to be an engineer or a scientist when I grow up, but I probably will not get the chance.—
34. I won't have as good opportunities when I grow up as many of my classmates.—
35. I wish my parents were not so strict with me, and more like the parents of many of my classmates in this way.—
36. I wish my parents were a little more strict with me, like the parents of many of my classmates.—
37. I wish my father and mother were better educated, like the parents of many of my classmates.—
38. I wish my father had as good a job as many of my classmate's fathers.—
39. I wish I could go on dates the way many of my classmates do.—
Now write down one wish that you have felt strongly about this past year.

PART VII. SOCIAL VALUES AND FEELINGS

Please answer each question by making a check in the space next to agree or disagree. There are no right or wrong answers. Just report your opinion.
40. Watching television programs such as "Sugarfoot" and the "Donna Reed Show" and "Dobie Gills" is boring or dull and a waste of time:
(0)—Agree.
(1)—Disagree.
41. Having a coke in a drugstore with other boys and girls after school or on a week end is dull and a waste of time:
(0)—Agree.
(1)—Disagree.
42. Watching school athletic contests is boring and a waste of time:
(0)—Agree.
(1)—Disagree.
43. Watching school basketball or football games is fun:
(1)—Agree.
(0)—Disagree.
44. Television programs such as "Cheyenne" and "National Velvet" and "Lassie" are fun to watch:
(1)—Agree.
(2)—Disagree.
45. The people who get the best jobs when they grow up are usually the people who have friends who do favors for them, rather than the people who are best trained or educated:
(0)—Agree.
(1)—Disagree.
46. Teachers give their praise and recognition to the students who find a way to become their special favorities, whether these students are good workers in school or not:
(0)—Agree.
(1)—Disagree.
47. Most teachers do not really like to help students:
(0)—Agree.
(1)—Disagree.

48. Teachers give their praise and recognition to the students who work the hardest and learn the most:
(1)—Agree.
(0)—Disagree.
49. The popular children in any school are the ones who have earned the respect and admiration of other students:
(1)—Agree.
(0)—Disagree.
50. Teachers have such different ideas about what you are supposed to learn in school that it is impossible to get a clear idea of what is best:
(0)—Agree.
(1)—Disagree.
51. People have such different ideas about what is right and wrong that you can't ever get clear ideas on this question:
(0)—Agree.
(1)—Disagree.
52. Once some teachers decide that a certain boy or girl is "bad" or a "trouble-maker," there is nothing you can do to change their minds:
(0)—Agree.
(1)—Disagree.
53. Teachers can usually tell quite well who is learning a lesson and who is not:
(1)—Agree.
(0)—Disagree.
54. Most parents have very clear ideas about how their children should act on dates and about matters like kissing:
(1)—Agree.
(0)—Disagree.
55. People in any town have a lot to say about how their town government is run:
(1)—Agree.
(0)—Disagree.
56. The children and adults in any town can help the police do a good job of enforcing the law:
(1)—Agree.
(0)—Disagree.
57. Students in junior high schools never have any say or influence in what they are taught in their classes.
(0)—Agree.
(1)—Disagree.
58. So many other people voted in the national election last fall that it didn't matter to me whether my parents voted or not.
(0)—Agree.
(1)—Disagree.
59. If a group of children decide they do not like you, there is nothing much you can do to change their minds:
(0)—Agree.
(1)—Disagree.

PART VIII. WAYS OF DISCIPLING YOUNG PEOPLE

Below are various ways by which many parents discipline children and young people. *Please answer each question by checking the choice which best tells how your parents have disciplined you during the last 2 years.* Answer each question for your mother and your father separately.

Do your parents take away your allowance?
61. Father:
(0)—Never.
(1)—Very seldom.
(2)—Sometimes.
(3)—Frequently.
62. Mother:
(0)—Never.
(1)—Very seldom.
(2)—Sometimes.
(3)—Frequently.

Do your parents refuse to speak to you?

63. Mother:
(1)—Very seldom.
(2)—Sometimes.
(3)—Frequently.
(0)—Never.
64. Father:
(2)—Sometimes.
(0)—Never.
(3)—Frequently.
(1)—Very seldom.

Have your parents slapped you or given you spankings?

65. Mother:
(3)—Frequently.
(2)—Sometimes.
(0)—Never.
(1)—Very seldom.
66. Father:
(2)—Sometimes.
(3)—Frequently.
(1)—Very seldom.
(0)—Never.

Do your parents forbid you to do something that you were especially planning on doing?

67. Father:
(3)—Frequently.
(2)—Sometimes.
(0)—Never.
(1)—Very seldom.
68. Mother:
(3)—Frequently.
(2)—Sometimes.
(0)—Never.
(1)—Very seldom.

Do your parents tell you to leave home or to find a new home if you can't be better?

69. Mother:
(1)—Very seldom.
(2)—Sometimes.
(0)—Never.
(3)—Frequently.
70. Father:
(2)—Sometimes.
(0)—Never.
(3)—Frequently.
(1)—Very seldom.

Do your parents spank you with a stick, belt, hairbrush, or things other than their hands?

71. Mother:
(1)—Very seldom.
(0)—Never.
(3)—Frequently.
(2)—Sometimes.
72. Father.
(0)—Never.
(3)—Frequently.
(2)—Sometimes.
(1)—Very seldom.

Do your parents take away some special privileges?

73. Mother:
(2)—Sometimes.
(3)—Frequently.
(0)—Never.
(1)—Very seldom.
74. Father:
(2)—Sometimes.

(3)—Frequently.
(0)—Never.
(1)—Very seldom.
Do your parents say they don't love you or warn you that they will stop loving you?
75. Father:
(3)—Frequently.
(2)—Sometimes.
(0)—Never.
(1) Very seldom.
76. Mother:
(2)—Sometimes.
(3)—Frequently.
(1)—Very seldom.
(0)—Never.
Have your parents beat you up (using their fists, etc.)?
77. Father:
(2)—Sometimes.
(0)—Never.
(3)—Frequently.
(1)—Very seldom.
78. Mother:
(3)—Frequently.
(2)—Sometimes.
(1)—Very seldom.
(0)—Never.

Mr. PELL. Mr. President, I ask for the yeas and nays on section (b).
The yeas and nays were ordered.
The PRESIDING OFFICER. Do Senators yield back their time?
Mr. STEVENS. Mr. President, a parliamentary inquiry.
The PRESIDING OFFICER. The Senator will state it.
Mr. STEVENS. Is this amendment still open to amendment?
The PRESIDING OFFICER. Is the amendment open to amendment?
Mr. STEVENS. Yes.
The PRESIDING OFFICER. The Senator from New York has requested the division of his amendment, and section (b) will be voted on separately. All the rest will be voted on by voice vote first.
Mr. STEVENS. Is it in order to submit an amendment to delete subsection (c) at this time.
The PRESIDING OFFICER. That would be in order now.
Mr. STEVENS. I send such an amendment to the desk.
The PRESIDING OFFICER. Have the Senator from New York and the Senator from Rhode Island yielded back their time?
Mr. PELL. My recollection is not acute on that. What does the Record show?
The PRESIDING OFFICER. Does the Senator yield back his time?
Mr. PELL. I yield it back.
Mr. BUCKLEY. I yield back the remainder of my time.
The PRESIDING OFFICER. The clerk will state the amendment of the Senator from Alaska.
The assistant legislative clerk read as follows:
On page 4, line 14, delete subsection (c).
Mr. STEVENS. Mr. President, I again applaud what the Senator from New York is trying to do, but I think any proposal that has to have so many amendments on the floor to try to perfect the original intent is a measure that should not be passed.
Subsection (a) is a good subsection. Subsection (b), as I read it, on protection of personal data, gives the Secretary and the schools the right to protect personal data under any regulations that are necessary to control the use, dissemination, or protection of such data.
Subsection (c) is not necessary, and what is more, again I point out that it would harm the students. It would prevent those with legitimate interests from going to a school and getting the information that is necessary. It would prevent the Senator from New York from deciding to recommend a student for some national award without going and telling him, if he was over 18. One would have to have his consent to get any information from his record.

It would prevent a probation officer—notwithstanding the argument of my good friend from Delaware, I still have faith in the probation system, and I think the probation officer ought to be able to go in and get the information necessary not only when a student is subject to a juvenile proceeding, but in order to continue the work that he has to do during the period before a juvenile is sentenced. Many times they have to keep up with what they are doing. It is a probation officer's duty to find out what he is doing in school. This would even prevent a probation officer from getting attendance data. I cannot understand us putting such a cloak of secrecy around a student.

On the other hand, subsection (c), as I understand it, gives the school authorities complete authority to adopt appropriate regulations. That would be subject to the Administrative Procedures Act. Everyone concerned would be involved in a hearing.

This has not been the subject of hearings by committee, and I do not think it is the kind of thing that ought to be passed on the floor of the Senate without further consideration. Therefore, to save time, I ask the deletion of that section.

I yield back the remainder of my time.

Mr. PELL. Mr. President, I think there is merit in what the Senator from Alaska says, and I would vote the same way. I yield back the remainder of my time.

Mr. BUCKLEY. Mr. President, I ask for the yeas and nays.

The yeas and nays were ordered.

The PRESIDING OFFICER. Does the Senator from Rhode Island yield back his time?

Mr. PELL. Mr. President, I yield back the remainder of my time.

The PRESIDING OFFICER (Mr. Nunn). All time has now been yielded back——

Mr. ERVIN. Mr. President, a parliamentary inquiry. What are we voting on?

The PRESIDING OFFICER. On the amendment of the Senator from Alaska (Mr. Stevens) to strike section (c).

Mr. BUCKLEY. Mr. President, I do not believe I yielded back my time yet.

The PRESIDING OFFICER. On the Stevens amendment, the Senator from New York does not have any time.

Mr. STEVENS. Mr. President, I ask unanimous consent that the Senator from New York (Mr. Buckley) may have 5 minutes to respond. I think that is only fair.

The PRESIDING OFFICER. Is there objection to the unanimous-consent request of the Senator from Alaska? The Chair hears none, and it is so ordered.

Mr. BUCKLEY. Mr. President, if the distinguished Senator from North Caroline (Mr. Ervin) wants to address himself to that point, I yield to him to do so.

Mr. President, I would merely say that the area addressed by the Senator from Alaska (Mr. Stevens) is but one area. Probation reports have also been leaked to the FBI, and other files as well. This is an area of extreme sensitivity. I do not believe that, absent appropriate court orders, this information should be made available.

Mr. ERVIN. Mr. President, section (d), as I understand it, provides that—

"The Secretary shall adopt appropriate regulations to protect the rights of privacy of students and their families in connection with any surveys or data-gathering activities conducted, assisted, or authorized by the Secretary . . ."

I do not see any objection to protecting the privacy of children. I do not see that they should be made guinea pigs by social scientists. That is why I support the bill.

Mr. STEVENS. Mr. President, with all due respect to the distinguished Senator from North Carolina, my amendment is to delete section (c), not (d).

Mr. BUCKLEY. Mr. President, I yield back the remainder of my time.

The PRESIDING OFFICER. All time on this amendment has now been yielded back.

The question is on agreeing to the amendment of the Senator from Alaska (Mr. Stevens) to strike section (c).

On this question the yeas and nays have been ordered, and the clerk will call the roll.

The assistant legislative clerk called the roll.

Mr. ROBERT C. BYRD. I announce that the Senator from Arkansas (Mr. Fulbright), the Senator from Alaska (Mr. Gravel), the Senator from South Carolina (Mr. Hollings), the Senator from Hawaii (Mr. Inouye), the Senator from Utah (Mr. Moss), the Senator from West Virginia (Mr. Randolph), the Senator from Alabama (Mr. Sparkman), the Senator from Texas (Mr. Bentsen), and the Senator from Missouri (Mr. Symington) are necessarily absent.

I further announce that, if present and voting, the Senator from West Virginia (Mr. Randolph) would vote "yea."

Mr. GRIFFIN. I announce that the Senator from Utah (Mr. Bennett), the Senator from Kentucky (Mr. Cook), the Senator from Florida (Mr. Gurney), the Senator from New York (Mr. Javits), and the Senator from Illinois (Mr. Percy) are necessarily absent.

I also announce that the Senator from Nebraska (Mr. Curtis), and the Senator from Arizona (Mr. Goldwater) are absent on official business.

I further announce that, if present and voting, the Senator from Nebraska (Mr. Curtis) would vote "nay."

The result was announced—yeas 35, nays 49, as follows:

[No. 194 Leg.]

YEAS—35

Aiken	Haskell	Nunn
Bayh	Hathaway	Packwood
Bible	Huddleston	Pell
Byrd, Robert C.	Jackson	Proxmire
Cannon	Kennedy	Ribicoff
Clark	Magnuson	Stennis
Cotton	McGee	Stevens
Dominick	McGovern	Stevenson
Eagleton	McIntyre	Taft
Griffin	Metcalf	Talmadge
Hart	Metzenbaum	Williams
Hartke	Nelson	

NAYS—49

Abourezk	Domenici	Mondale
Allen	Eastland	Montoya
Baker	Ervin	Muskie
Bartlett	Fannin	Pastore
Beall	Fong	Pearson
Bellmon	Hansen	Roth
Biden	Hatfield	Schweiker
Brock	Helms	Scott, Hugh
Brooke	Hruska	Scott, Wiliam L.
Buckley	Hughes	Stafford
Burdick	Humphrey	Thurmond
Byrd, Harry F., Jr.	Johnston	Tower
Case	Long	Tunney
Chiles	Mansfield	Weicker
Church	Mathias	Young
Cranston	McClellan	
Dole	McClure	

NOT VOTING—16

Bennett	Gravel	Percy
Bentsen	Gurney	Randolph
Cook	Hollings	Sparkman
Curtis	Inouye	Symington
Fulbright	Javits	
Goldwater	Moss	

So Mr. Stevens' amendment was rejected.

Mr. CRANSTON. Mr. President, the Senator from New York (Mr. Buckley) has proposed an amendment regarding the confidentiality of student records and requiring parental consent for certain school activities that causes me some concern.

The first portion of the amendment seeks to guarantee the right of access and review of a student's school records, by parents and by students—if 18 years of age or over—and prevent the disclosure of such records to most third parties without parental or student consent.

I would wholeheartedly support this portion of the Senator's amendment. It seems to me that it seeks to preserve a right to confidentiality of records of student academic and personal performance that should be guaranteed. I would

point out, however, that in my State of California, this right of access and review is presently guaranteed under the California Public Records Act.

The section of the amendment that deals with "parental consent," however, causes me serious concern.

First, I question the advisability of the Congress enacting legislation that, in effect, would thwart a State's compulsory attendance laws. Under this amendment, a parent may refuse to have his child attend a class if, after notification, the parent finds the content of the course or activity to be objectionable. While I do not object to "parental consent," I do question Federal interference in what I believe to be a question that should be decided by locally elected school officials, rather than the Federal Government.

Second, subsection (b)(2) of the amendment would require parental consent for students—and I quote:

"To participate in any project, program, or course, the primary purpose or principal effect of which is to affect or alter the personal behavior or personal values of a student, or to explore and develop teaching techniques or courses primarily intended to affect such behavior and values."

Mr. President, this language is breathtaking in its sweeping generalities. How do you determine in advance, and provide notificaton to the parent, of classroom activities that might bear on the values of a student? A course in American history, for example, that discusses contemporary American ethics in the light of Watergate could be construed as tending to "affect the personal values" of a student. Or, how do you go about discouraging violent or overly aggressive behavior without tending to "alter the personal behavior" of a student?

These are serious questions, Mr. President, that we cannot take lightly. Because the penalty for even accidental transgression of these Federal directives is the total loss of Federal funding to any educational institution—public or private, preschool through postsecondary—that is found "out of compliance."

Finally, Mr. President, the amendment directs the Secretary of Health, Education, and Welfare with the responsibility for—and again, I quote:

"Investigating, processing, reviewing, and adjudicating violations of the provisions of this section and complaints."

Frankly, I question the wisdom of charging a Federal agency with the power to probe the questions that would have to be probed in order to investigate complaints of alleged violations of the act. Such questions could include:

Was the purpose of the course to affect the values of the child, or were they affected accidentally, or at all?

Even if the purpose of the course was not to alter the values of the child, did it have the effect of altering the values of the child?

What were the values of the child before they were "altered"?

Mr. President, I believe my point is obvious: This section of the Senator's amendment brings the Federal Government and its agencies dangerously close to deciding issues of academic and personal freedom that should be in the hands of local and State school officials, and the people who elected them, not the Federal Government.

I do not believe the Senate of the United States should take any action that could be legitimately construed as having the primary effect of circumventing local control of curriculum and school practices, discouraging innovation, or stifling educational reform.

For these reasons, and because I support the major premise of the Senator's amendment, I would hope he would consider deleting the section of the amendment to which I have referred.

The PRESIDING OFFICER. The question now occurs on the first part of the amendment of the Senator from New York.

Mr. PELL. The vote is now on section (b), is it not? What is the parliamentary situation?

The PRESIDING OFFICER. The question now occurs on all of the amendment except section (b).

The amendment was agreed to.

The PRESIDING OFFICER. The question now occurs on section (b) of the amendment. On this question, the yeas and nays have been ordered, and the clerk will call the roll.

Mr. MANSFIELD. Mr. President, what are we voting on?

The PRESIDING OFFICER. On section (b) of the Buckley Amendment.

The second assistant legislative clerk proceeded to call the roll.

Mr. ERVIN. Mr. President, precisely what is this?

The PRESIDING OFFICER. The rollcall is now in progress.

Mr. HUMPHREY. Mr. President, a parliamentary inquiry.

The PRESIDING OFFICER. The question is on the adoption of section (b) of the Buckley amendment.

Mr. HUMPHREY. Up and down on section (b)?

The PRESIDING OFFICER. That is correct.

The question is on the adoption of section (b) of the Buckley amendment.

The clerk will call the roll.

The second assistant legislative clerk resumed and concluded the call of the roll.

Mr. ROBERT C. BYRD. I announce that the Senator from Texas (Mr. Bentsen), the Senator from Arkansas (Mr. Fubright), the Senator from Alaska (Mr. Gravel), the Senator from South Carolina (Mr. Hollings), the Senator from Hawaii (Mr. Inouye), the Senator from Utah (Mr. Moss), the Senator from West Virginia (Mr. Randolph), the Senator from Alabama (Mr. Sparkman), and the Senator from Missouri (Mr. Symington) are necessarily absent.

I further announce that, if present and voting, the Senator from West Virginia (Mr. Randolph) would vote "nay."

Mr. GRIFFIN. I announce that the Senator from Utah (Mr. Bennett), the Senator from Kentucky (Mr. Cook), the Senator from Florida (Mr. Gurney), the Senator from New York (Mr. Javits), the Senator from Oregon (Mr. Packwood), and the Senator from Illinois (Mr. Percy) are necessarily absent.

I also announce that the Senator from Nebraska (Mr. Curtis) and the Senator from Arizona (Mr. Goldwater) are absent on official business.

I further announce that, if present and voting, the Senator from Nebraska (Mr. Curtis) would vote "yea."

The result was announced—yeas 40, nays 43, as follows:

[No. 195 Leg.]

YEAS—40

Baker	Fannin	Pastore
Bartlett	Fong	Pearson
Beall	Griffin	Proxmire
Bellmon	Hansen	Roth
Brock	Helms	Scott, Hugh
Buckley	Hruska	Scott, William L.
Byrd, Harry F., Jr.	Huddleston	Stennis
Byrd, Robert C.	Johnston	Taft
Chiles	Mansfield	Thurmond
Church	McClellan	Tower
Dole	McClure	Weicker
Domenici	Metcalf	Young
Eastland	Montoya	
Ervin	Nelson	

NAYS—43

Abourezk	Hart	Metzenbaum
Aiken	Hartke	Mondale
Allen	Haskell	Muskie
Bayh	Hatfield	Nunn
Bible	Hathaway	Pell
Biden	Hughes	Ribicoff
Brooke	Humphrey	Schweiker
Burdick	Jackson	Stafford
Cannon	Kennedy	Stevens
Case	Long	Stevenson
Clark	Magnuson	Talmadge
Cotton	Mathias	Tunney
Cranston	McGee	Williams
Dominick	McGovern	
Eagleton	McIntyre	

NOT VOTING—17

Bennett	Gravel	Packwood
Bentsen	Gurney	Percy
Cook	Hollings	Randolph
Curtis	Inouye	Sparkman
Fulbright	Javits	Symington
Goldwater	Moss	

So section (b) of Mr. Buckley's amendment (No. 1289) was rejected.

Mr. PELL. Mr. President, I move to reconsider the vote by which the amendment was rejected.

Mr. EAGLETON. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

Several Senators addressed the Chair.

The PRESIDING OFFICER. The Senator from Colorado is recognized.

Mr. DOMINICK. I yield to the Senator from California.

The PRESIDING OFFICER. The Senator from California is recognized.

Mr. DOMINICK. Mr. President, I yield to the Senator from Missouri.

Mr. EAGLETON. Mr. President, I ask unanimous consent that James Murphy and Marsha McCord be accorded the privileges of the floor during consideration of the education bill.

The PRESIDING OFFICER. Without objection, it is so ordered.

[From the Federal Register, May 30, 1974]

PROTECTION OF HUMAN SUBJECTS

REGULATIONS OF DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE

In the Federal Register of October 9, 1973 (38 FR 27882), a notice of proposed rulemaking was published in which it was proposed to amend subtitle A of the Department's regulations to codify, with some changes, an existing Departmental policy set forth in Chapter 1–40 of the DHEW Grants Administration Manual. These regulations would provide that no activity involving any human subjects at risk supported by a DHEW grant or contract shall be undertaken unless a committee of the applicant or offering organization has reviewed and approved such activity and submitted to DHEW a certification of such review and approval. In addition any organization receiving a grant or contract must establish a mechanism to provide for continuing review of the supported activity to insure its continued acceptability. The notice provided for the filing of comments within 30 days, ending November 8, 1973.

Comments were received from more than 140 representatives of grantee and contractor organizations, from approximately 20 public groups or organizations, and from over 40 individuals. They include over 500 criticisms of individual sections of the proposed rules. These comments and the Department's conclusions are principally as follows:

A. The applicability and scope of the policy were challenged by several respondents. Suggestions included limiting the policy to physical risks only, differentiation of biomedical risks from behavioral risks, expanding the policy to protect all persons regardless of the nature of the risk or source of support, and unequivocal limitation of the policy to DHEW grants and contracts as contrasted to other organizational activities. Requests were also made for the provision of special exemptions for subject groups such as prisoners, academic colleagues, students, and laboratory personnel; or exemptions for specific procedures such as those involving manipulation of the diet within normal ranges, the taking of blood and urine samples, surgical and autopsy specimens, and the use of hair, nail clippings, and placental materials.

It was also proposed that the policy deal specifically with certain subjects such as the prisoner, the child, the fetus, the abortus, and the candidate for sterilization or psychosurgery.

The Department, having considered these frequently conflicting recommendations, concludes that the language of the regulations should be changed to emphasize their concern with the risks involved in research, development, and related activities. It concludes that the arguments advanced for specifically including for exempting certain activities and procedures from the scope of the policy frequently reflect considerations applicable only to individual projects or conditions in particular institutions and lack broad applicability. It therefore seems appropriate to reserve to the Secretary the right to designate activities which necessarily fall within the scope of these regulations or to which the regulations are inapplicable. Such designations will be made only following careful study and through publication in the Federal Register. These changes are incorporated in § 46.1. At the same time it should be noted that the Department is now developing policies dealing more specifically with research, development, and related activities involving the prisoner, the child, the fetus, the abortus, and institutionalized individual with mental disability. The Department intends

to issue one or more notices of proposed rule making the Federal Register no later than July 30, 1974, dealing with these subjects. Policies are also under consideration which will be particularly concerned with the candidate for psychosurgery, the candidate for sterilization and, separately, with the subject of social science research.

B. Criticisms of the basic policy statement centered about the requirement that organizational committee review determine "that the risks to an individual are outweighed by the potential benefits to him, or by the importance of the knowledge to be gained." Suggestions included inserting the word "significant" before "risks" and adding after the word "gained" such phrases as "provided the experimental procedure accords decent respect for the opinion of mankind" and "or by the potential benefit to society." Objections were also raised concerning the requirement that informed consent be qualified as "adequate" and to the omission of a requirement that it be "legally effective." It was also argued that the sole purpose of the reviews should be to determine that the subject is fully informed.

The Department, having considered these comments, concludes that the addition of the term "significant" would tend to weaken, not to strengthen the requirement, and that the intent of the proposed change is better served by provisions in § 46.1 giving the Secretary authority to designate activities, including methods and procedures, to which the policy is inapplicable. The suggested changes in the risk-benefit clause appear to be more admonitory than substantive. Objections to the use of the term "adequate" appeared to be based on an assumption that the term was used in the sense of "barely sufficient" rather than "lawfully and reasonably." The Department concurs that the requirement is strengthened by the substitution of the phrase "legally effective." It does not agree that the sole purpose of the review should be to determine that the subject is fully informed. It is essential that the committee, representing a wide spectrum of those expert professional skills essential to a clear recognition of an activity's inherent risks and probable benefits, carefully weigh such risks and benefits before determining that the benefits favor a decision to allow the subject to accept these risks. It is also important that the committee determine that the subject will receive adequate protection against known risks. These conclusions and certain editorial changes are reflected in § 46.2.

C. Objections were raised to several of the definitions incorporated into the regulations: (i) since the DHEW may make grants to certain Federal agency components only on the same terms as to non-Federal institutions, it was suggested that the term "Organization" should be expanded to include Federal agencies, (ii) objections were also raised to the term "sociological harm" as meaningless, and to the use of the term "harm" rather than the common legal term "injury," (iii) the definition of "informed consent" was challenged on several counts. It was suggested that the definition should be couched in terms similar to those of the Nuernberg Code which provides that "the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice without the intervention of any element of force, fraud, deceit, duress, overreaching, or other ulterior form of constraint or coercion." It was also suggested (iv) that the requirement for an instruction that the subject be free to withdraw his consent be amended to read additionally "without prejudice to his future care."

Additional suggestions included: (v) add to each of the elements of informed consent the initial phrase "full and fair." (vi) eliminate the requirement for a description of "any appropriate alternative procedures" since there might not be any such procedures; (vii) add a requirement that the patient be informed of alternatives if he is unable or refuses to continue as a research subject; and (viii) that patients be informed of the consequences should the research fail.

The recommendations having been duly considered it is concluded that suggested changes (i) through (iv) should be incorporated into the regulations with some editorial changes, particularly elimination of the phrase "to his future care" from the addition suggested in (iv) above. Prejudice could extend to other matters such as reimbursement of expenses, compensation, employment status, etc. The remaining recommendations (v–viii) are considered for the most part redundant and additional changes appear unnecessary.

These conclusions are reflected in § 46.3. Definitions of certain additional terms have been included as required by changes made elsewhere in this part.

D. With regard to the submission of assurances, criticisms were voiced concerning the requirement that the organization report to DHEW any emergent problems. Respondents emphasized that the term "emergent problems" was vague and, if strictly interpreted, could lead to enormous amounts of unnecessary paperwork at great cost both to the organization and to the DHEW. Respondents were also critical of the requirement for "immediate notification" and questioned the value of such data.

These comments having been considered, it is concluded that they have some merit. The requirement has been modified, removed from its original position in the regulations, and inserted elsewhere. The terms "emergent problems" and "immediate notification" have been eliminated. These changes are reflected in §§ 46.4, 46.6(d), and 46.7(e).

Comments were also concerned with the proposed requirement that no "committee or quorum of a committee shall consist entirely of employees of the organization." Respondents stated that in most institutions it would be difficult, and in some impossible, to find, attract, and hold qualified, interested nonemployees; that the absence of such a person from a quorum could block consideration of unexpected problems, make difficult the scheduling of meetings to meet DHEW imposed deadlines for the preparation of grants and contracts, and invest such persons with "absentee veto" power. Also, that the provision would deny reasonable compensation of outsiders currently or possibly serving on committees, and deny legal protection and the protection of organizational liability insurance to outsiders who were not in an employee status while serving on a committee subject to suit.

Most suggestions for alternate wordings of the provision would either drop the mandatory requirement for nonemployees, or suggest that the requirement be made optional, the choice to depend upon the judgment of the Secretary or the organizational committee as to whether or not such nonemployee representation was necessary. Other recommendations suggested that "nonemployee" be defined in terms of sole employment by the organization, full or part-time employment, or short-term employment. Some respondents suggested more restrictive requirements, providing that the nonemployee group be defined to include nonhealth professionals who would either represent population groups, or subject populations. Finally, objections were raised to the requirement that the committee be able to ascertain acceptability of the proposal in terms of community attitudes. It was suggested that such attitudes are vague, nebulous, and fluctuating and, since a wide range of communities may be involved, impossible of representation.

These comments having been considered, it is concluded that the requirement for nonemployee members on organizational committees is an essential protection against the development of insular or parochial committee attitudes, that it assists in maintaining community contacts, and would augment the credibility of the committee's independent role in protection of the subject. However, it is agreed that the requirement that nonemployees be included in quorums appears to be impractical, and that the requirement should not be so phrased as to prevent a committee member from being considered an employee within the scope of the organization's liability coverage or legal protection. The arguments against committee consideration of community attitudes are considered generally to be offset by equally strong reasons for taking these attitudes into consideration. It should be emphasized that the term "community" is intended to be applied in the sense of the larger community served by the organization, not necessarily the smaller community involved in a particular supported activity or project, that this is a requirement for overall committee membership, and not a requirement that must be varied proposal by proposal. The Department's conclusions are reflected by § 46.6(b) (2), (4), (5), and (6).

E. Comments on the requirements for special assurances were largely editorial. It is concluded that changes should be made so as to insure better agreement between the wording of these requirements and those for general assurances. These changes are reflected in § 46.7.

F. Comments on the obligation to secure informal consent pointed out that there appeared to be conflict between this requirement and the section on documentation or informed consent, since the latter permits some modification of written procedures. Other respondents suggested changes in language similar to that found in the Nuernberg Code and already incorporated into the definition of informed consent in § 46.3(c), or sought changes to define conditions under which substituted consent could be obtained on behalf of individuals who are

incompetent, either because of age or mental incapacity, to consent for themselves. Among other matters it was suggested that such substituted consent should only be given by a court of competent jurisdiction.

These comments having been considered, it is concluded that there is no substantial conflict between this section and the documentation requirements, that the suggestion of inclusion of the Nuernberg Code language has been met elsewhere, and that problems relating to participation by minors, the mentally ill and mentally retarded, and by prisoners and others are already the subject of a draft proposed rulemaking (See 38 FR 31738 et seq.).

G. Objections were raised to the clause prohibiting the use of exculpatory language on the grounds that it makes organizational review committees subject to suit as agents of the organization and negates any protection offered by organizational liability insurance. The Department's Office and General Counsel has been able to find no legal support for this unsubstantiated assertion concerning limitations on insurance protection and has advised that the use of exculpatory language should be prohibited as a matter of public policy.

H. Comments on documentation of informed consent centered largely about the term "authorized representative." Suggestions included substitution of the term "legal representative" or use of "authorized representative," variously defined with regard to his association with any organization having custody of the subject, or proposing to seek the subject's consent, or having simultaneous responsibility for the subject's health and welfare. Additional comments focused on the concept of the "auditor-witness," emphasizing the impracticability of implementing such a concept in mass surveys and in emergency situations. Others raised doubts as to the need for written consent procedures in connection with low risk procedures. Several respondents suggested that it be required that the subject receive a copy of the completed consent document. One respondent suggested a 24-hour lapse between the time of receiving information and the time of giving consent.

The Department, having considered these comments, concludes that the substitution of "legally authorized representative," as defined in § 46.3(h) for "authorized representative" and that the provisions for modification of either of the two primary methods of informed consent allow all necessary flexibility for the development of consent procedures. The suggestions that a copy of the completed consent document be provided to the subject, and that provision be made for a 24-hour waiting period, are matters to be left to the discretion of the organization. The necessary changes have meen made in § 46.10.

I. Various commentators raised questions with regard to the review and approval of assurances. An additional section describing evaluation and disposition of assurances has been inserted as § 46.10. The language of this section is consistent with current policy as stated in DHEW Grants Administration Manual Chapter 1–40.

J. A large number of organizations were concerned with the proposed requirement that organizational review and approval be completed and certified prior to the submission of proposals to DHEW. Although the majority of respondents favored retaining the present policy, an almost equal number suggested that they could complete all of their reviews within a few weeks following submission to DHEW. Emphasis was laid on the need for time for revision, resubmission, and review of proposals found unacceptable at the time of first submission.

A few public groups commended this requirement as a substantial improvement over present policy which, in their opinion, presented a local committee with an impossible task in questioning a project which had already received review and approval at a national level.

These comments having been considered, it is concluded that the right to relax this requirement, and to extend a grace period for completion and certification of review after submission of the proposal should be reserved to the Secretary. In no event will processing of a proposal by DHEW be completed until such certification has been received by DHEW. These conclusions are reflected by changes in §§ 46.11 and 46.12.

By separate notice, the Department will provide that for a period of one year from the effective date of these regulations, organizations having approved general assurances may give proposals review and approval after submission to DHEW provided that such certification is received by DHEW no later than 30 days following the deadline for which the proposal was submitted, or, if no deadline is specified, 30 days following the submission date of the proposal. Organizations not having a significant number of concurrent DHEW-supported

activities must submit a special assurance and certification of review and approval to DHEW within 30 days of the date of a letter requesting such submission.

K. With regard to the section on proposals lacking definite plans for involvement of human subjects, a majority of respondents objected to the provision calling for submission of completed plans to DHEW for its prior review and approval. Commentators pointed out the problems inherent in delay in the implementation of short-term projects, and the problems to be encountered by DHEW in providing adequate review of such projects on a demand basis. Suggestions included: (i) a requirement for institutional review without submission to DHEW; (ii) review with notification to DHEW; and (iii) review and submission of plans to DHEW, such plans to be implemented if no DHEW objections were interposed within 30 days of submission.

These comments having been considered, it is concluded that the proposed requirement for DHEW review of final stage plans for previously reviewed and approved proposals is impractical and unrealistic. Section 46.13 has been rewritten to require institutional review and approval, and for certification of such action to DHEW prior to involvement of human subjects.

L. Comments on the requirements for organizational and DHEW review of proposed plans to involve human subjects in activities initially funded with the understanding that human subjects would not be involved, were similar to those described in the preceding paragraphs. Again, respondents objected that the requirement for DHEW review would unnecessarily delay research, create unnecessary paperwork, and create substantial fiscal and administrative burdens. Suggestions were made for submission of plans to DHEW, such plans to be implemented if no DHEW objections were interposed within 30 days of submission.

These comments, having been considered, the Department sees no viable alternative to the rules as proposed. Where the DHEW is aware of the intent to involve human subjects, as in the type of proposal described in § 46.13, it can take into consideration the probable nature of the involvement and the probable risks and benefits to the subjects. If necessary it may acquire additional information prior to review, or make any such approval contingent on submission of final stage plans. These opportunities are not available to DHEW if it is not informed in advance of potential involvement of human subjects.

No changes have been made in § 46.14.

M. In order to emphasize the Secretary's authority to conduct further evaluation of proposed activities involving human subjects and to disapprove, defer, or approve such proposals, and to impose conditions on such approvals, § 46.15 has been inserted. The language of this section is consistent with current policy in DHEW Grants Administration Manual Chapter 1–40.

N. Comments on the proposed regulations governing cooperative activities were in frequent conflict. Alternative suggestions included: (i) changes making it possible for a prime contractor or grantee to assume all responsibility for the conduct of work by cooperating organizations, (ii) changes which would eliminate all responsibility by the prime contractor or grantee for work done by cooperating organizations, (iii) changes which would discourage any requirement for submission for assurance by cooperating organizations, (iv) inclusion of language limiting a prime contractor or grantee responsibility for work performed by a subcontractor, (v) inclusion of language spelling out the instruments and documents to be provided by the cooperating organization, (vi) elimination of any requirement that would require a domestic contractor or grantee to be aware of local laws and community attitudes in foreign countries.

The Department having reviewed these comments, concludes that these often conflicting suggestions fail to provide any better alternatives than the regulations as proposed. There appears to be no reasonable alternative to requiring the prime contractor to remain responsible for safeguarding the rights and welfare of subjects, either directly under the provision of his own assurance, or through the mechanisms provided by assurances submitted by cooperating organizations. The proposed regulations permit a contractor or grantee some flexibility to meet the requirements of the policy. The proposed rules are incorporated unchanged in § 46.16.

O. Requirements for the submission of investigational new drug (IND) numbers prior to issuance of an award were criticized on several counts. One respondent felt that the regulations would make it difficult if not impossible to obtain DHEW support for studies leading to the development of a new drug. Not all compounds requiring IND's are actual drugs under development, but are em-

ployed for other purposes. Another respondent pointed out that the pertinent FDA regulations (21 CFR 130.3(a)(2)) make no reference to the IND number, but require a 30-day delay period prior to use of drugs in human subjects.

These comments having been considered, the Department agrees that references to the IND number should be replaced by reference to the FDA 30-day delay requirement. The Department does not agree that a requirement for submission of identification on IND's would cause undue delay in studies preliminary to submission of an IND exemption, since such studies are necessarily conducted in animal species. Section 46.18 has been altered accordingly.

P. With regard to retention of records, several respondents pointed out conflict between the proposed requirements for retention of records and recently published DHEW Administration of Grant regulations (45 CFR 74). Other comments reflected concern over the confidentiality of information which would be subject to DHEW inspection.

The Department, having reviewed these comments, concludes that the record retention and inspection requirements contained herein are redundant and should be deleted. A provision concerning confidentiality has been added. The appropriate changes have been made in § 46.19.

Q. Comments on the proposed sanctions for noncompliance with provisions of this part focused on two issues. (i) the absence of provisions for due process in the imposition of sanctions and, (ii) apparent intervention by DHEW in the employer-employee relationship in proposing to determine that an individual was no longer eligible to serve in the capacity of a principal investigator or in any similar capacity with respect to a DHEW grant or contract. Reference was made to clause 21 of the "General Provisions for Negotiated Cost-Reimbursement Type Contracts * * *" (HEW 315) which provides that "the Contractor agrees to assign (named personnel) * * * to the performance of work under this contract; and shall not remove or replace any of them * * *."

The Department has considered these comments and has concluded that actions under § 46.21(a), which refers to applicable grant and procurement regulations, would be subject to due process as provided for in these regulations. Section 46.21 (b) and (c) have been deleted, however, and replaced with a new provision which simply allows the Secretary to take into consideration past deficiencies of an institution or investigator, with regard to the protection of human subjects, in evaluating subsequent applications from that institution or involving that investigator. While it would appear from review of clause 21 of HEW 315 that it does not prevent the Department from effecting the removal of personnel from performance of work under a DHEW contract, it is agreed that the responsible organization should be a party to the notification and conference procedures necessary to the making of any such decision.

R. Several respondents suggested significant additions to the policy to provide among other matters for (i) the establishment of a National Commission to undertake a comprehensive investigation and study to develop basic ethical principles and guidelines which should govern biomedical and behavioral research, (ii) a conscience clause, prohibiting among other matters, discrimination in the employment of persons who, because of religious beliefs or moral convictions, perform, or refuse to perform a research or service activity prohibited by the entity on the basis of religious beliefs or moral convictions, and (iii) providing for the regulation of unapproved uses of approved drugs.

It is concluded that these suggestions would require changes not properly within the scope of these regulations and, in the case of regulation of unapproved uses of approved drugs, are the subject of regulations proposed as 37 FR 16503 on August 15, 1972.

S. Addition to the regulations of section of "Evaluation and disposition of assurances" has made unnecessary an earlier section on "Implementation and revision of assurances." Similarly, issuance of 45 CFR 74 has made unnecessary the earlier section entitled "Withholding of funds."

Effective date. This part shall become effective on July 1, 1974: *Provided, however,* That with respect to programs administered by the Office of Education and the National Institute of Education, this part shall become effective upon adoption or implementation in regulations issued by, respectively, the Commissioner of Education and the Director of the National Institute of Education, with the approval of the Secretary of Health, Education, and Welfare.

Dated: May 22, 1974.

CASPAR W. WEINBERGER,
Secretary.

Accordingly, Subtitle A of Title 45 of the Code of Federal Regulations is amended by adding a new Part 46, as follows:

Sec.

46.1 Applicability.
46.2 Policy.
46.3 Definitions.
46.4 Submission of assurances.
46.5 Types of assurances.
46.6 Minimum requirements for general assurances.
46.7 Minimum requirements for special assurances.
46.8 Evaluation and disposition of assurances.
46.9 Obligation to obtain informed consent; prohibition of exculpatory clauses.
46.10 Documentation of informed consent.
46.11 Certification, general assurances.
46.12 Certification, special assurances.
46.13 Proposals lacking definite plans for involvement of human subjects.
46.14 Proposals submitted with the intent of not involving human subjects.
46.15 Evaluation and disposition of proposals.
46.16 Cooperative activities.
46.17 Investigational new drug 30-day delay requirement.
46.18 Organization's executive responsibility.
46.19 Organization's records; confidentiality.
46.20 Reports.
46.21 Early termination of awards; evaluation of subsequent applications.
46.22 Conditions.

AUTHORITY: 5 U.S.C. 301

§ 46.1 Applicability.

(a) The regulations in this part are applicable to all Department of Health, Education, and Welfare grants and contracts supporting research, development, and related activities in which human subjects are involved.

(b) The Secretary may, from time to time, determine in advance whether specific programs, methods, or procedures to which this part is applicable place subjects at risk, as defined in § 46.3(b). Such determinations will be published as notices in the FEDERAL REGISTER and will be included in an appendix to this part.

§ 46.2 Policy.

(a) Safeguarding the rights and welfare of subjects at risk in activities supported under grants and contracts from DHEW is primarily the responsibility of the organization which receives or is accountable to DHEW for the funds awarded for the support of the activity. In order to provide for the adequate discharge of this organizational responsibility, it is the policy of DHEW that no activity involving human subjects to be supported by DHEW grants or contracts shall be undertaken unless a committee of the organization has review and approved such activity, and the organization has submitted to DHEW a certification of such review and approval, in accordance with the requirements of this part.

(b) This review shall determine whether these subjects will be placed at risk, and, if risk is involved, whether:

(1) The risks to the subject are so outweighed by the sum of the benefit to the subject and the importance of the knowledge to be gained as to warrant a decision to allow the subject to accept these risks;

(2) the rights and welfare of any such subjects will be adequately protected;

(3) legally effective informed consent will be obtained by adequate and appropriate methods in accordance with the provisions of this part; and

(4) the conduct of the activity will be reviewed at timely intervals.

(c) No grant or contract involving human subjects at risk shall be made to an individual unless he is affiliated with or sponsored by an organization which can and does assume responsibility for the subjects involved.

§ 46.3 Definitions.

(a) "Organization" means any public or private institution or agency (including Federal, State, and local government agencies).

(b) "Subject at risk" means any individual who may be exposed to the possibility of injury, including physical, psychological, or social injury, as a con-

sequence of participation as a subject in any research, development, or related activity which departs from the application of those established and accepted methods necessary to meet his needs, or which increases the ordinary risks of daily life, including the recognized risks inherent to a chosen occupation or field of service.

(c) "Informed consent" means the knowing consent of an individual or his legally authorized representative, so situated as to be able to exercise free power of choice without undue inducement or any element of force, fraud, deceit, duress, or other form of constraint or coercion. The basic elements of information necessary to such consent include:

(1) A fair explanation of the procedures to be followed, and their purposes, including identification of any procedures which are experimental;

(2) a description of any attendant discomforts and risks reasonably to be expected;

(3) a description of any benefits reasonably to be expected;

(4) a disclosure of any appropriate alternative procedures that might be advantageous for the subject;

(5) an offer to answer any inquiries concerning the procedures; and

(6) an instruction that the person is free to withdraw his consent and to discontinue participation in the project or activity at any time without prejudice to the subject.

(d) "Secretary" means the Secretary of Health, Education, and Welfare or any other officer or employee of the Department of Health, Eductaion, and Welfare to whom authority has been delegated.

(e) "DHEW" means the Department of Health, Education, and Welfare.

(f) "Approved asurance" means a document that fulfills the requirements of this part and is approved by the Secretary.

(g) "Certification" means the official organizational notification to DHEW in accordance with the requirements of this part that a project or activity involving human subjects at risk has been reviewed and approved by the organization in accordance with the "approved assurance" on file at DHEW.

(h) "Legally authorized representative" means an individual or judicial or other body authorized under applicable law to consent on behalf of a prospective subject to such subject's participation in the particular activity or procedure.

§ 46.4 Submission of assurances.

(a) Recipients or prospective recipients of DHEW support under a grant or contract involving subjects at risk shall provide written assurance acceptable to DHEW that they will comply with DHEW policy as set forth in this part. Each assurance shall embody a statement of compliance with DHEW requirements for initial and continuing committee review of the supported activities; a set of implementing guidelines, including identification of the committee and a description of its review procedures; or, in the case of special assurances concerned with single activities or projects, a report of initial findings of the committee and of its proposed continuing review procedures.

(b) Such assurance shall be executed by an individual authorized to act for the organization and to assume on behalf of the organization the obligations imposed by this part, and shall be filed in such form and manned as the Secretary may require.

§ 46.5 Types of assurances.

(a) *General assurances.* A general assurance describes the review and implementation procedures applicable to all DHEW-supported activities conducted by an organization regardless of the number, location, or types of its components or field activities. General assurances will be required from organizations having a significant number of concurrent DHEW-supported projects or activities involving human subjects.

(b) *Special assurances.* A special assurance will, as a rule, describe those review and implementation procedures applicable to a single activity or project. A special assurance will not be solicited or accepted from an organization which has on file with DHEW an approved general assurance.

§ 46.6 Minimum requirements for general assurances.

General assurances shall be submitted in such form and manner as the Secretary may require. The organization must include, as part of its general assurance, implementing guidelines that specifically provide for:

(a) A statement of principles which will govern the organization in the discharge of its responsibilities for protecting the rights and welfare of subjects. This may include appropriate existing codes or declarations, or statements formulated by the organization itself. It is to be understood that no such principles supersede DHEW policy or applicable law.

(b) A committee or committee structure which will conduct initial and continuing reviews in accordance with the policy outlined in § 46.2. Such committee structure or committee shall meet the following requirements:

(1) The committee must be composed of not less than five persons with varying backgrounds to assure complete and adequate review of activities commonly conducted by the organization. The committee must be sufficiently qualified through the maturity, experience, and expertise of its members and diversity of its membership to insure respect for its advice and counsel for safeguarding the rights and welfare of human subjects. In addition to possessing the professional competence necessary to review specific activities, the committee must be able to ascertain the acceptability of proposals in terms of organizational commitments and regulations, applicable law, standards of professional conduct and practice, and community attitudes. The committee must therefore include persons whose concerns are in these areas.

(2) The committee members shall be identified to DHEW by name; earned degrees, if any; position or occupation; representative capacity; and by other pertinent indications of experience such as board certification, licenses, etc., sufficient to describe each member's chief anticipated contributions to committee deliberations. Any employment or other relationship between each member and the organization shall be identified, i.e., full-time employee, part-time employee, member of governing panel or board, paid consultant, unpaid consultant. Changes in committee membership shall be reported to DHEW in such form and at such times as the Secretary may require.

(3) No member of a committee shall be involved in either the initial or continuing review of an activity in which he has a conflicting interest, except to provide information requested by the committee.

(4) No committee shall consist entirely of persons who are officers, employees, or agents, of, or are otherwise associated with the organization, apart from their membership on the committee.

(5) No committee shall consist entirely of members of a single professional group.

(6) The quorum of the committee shall be defined, but may in no event be less than a majority of the total membership duly convened to carry out the committee's responsibilities under the terms of the assurance.

(c) Procedures which the organization will follow in its initial and continuing review of proposals and activities.

(d) Procedures which the committee will follow (1) to provide advice and counsel to activity directors and investigators with regard to the committee's actions, (2) to insure prompt reporting to the committee of proposed changes in an activity and of unanticipated problems involving risk to subjects or others and (3) to insure that any such problems, including adverse reactions to biologicals, drugs, radioisotope labelled drugs, or to medical devices, are promptly reported to the DHEW.

(e) Procedures which the organization will follow to maintain an active and effective committee and to implement its recommendations.

§ 46.7 Minimum requirements for special assurances.

Special assurances shall be submitted in such form and manner as the Secretary may require. An acceptable special assurance shall:

(a) Identify the specific grant or contract involved by its number, if known; by its full title; and by the name of the activity or project director, principal investigator, fellow, or other person immediately responsible for the conduct of the activity. The assurance shall be signed by the individual members of a committee satisfying the requirements of § 46.6(b) and be endorsed by an appropriate organizational official.

(b) Describe the makeup of the committee and the training, experience, and background of its members, as required by § 46.6(b)(2).

(c) Describe in general terms the risks to subjects that the committee recognizes as inherent in the activity, and justify its decision that these risks are so outweighed by the sum of the benefit to the subject and the importance of the

knowledge to be gained as to warrant the committee's decision to permit the subject to accept these risks.

(d) Describe the informed consent procedures to be used and attach documentation as required by § 46.10.

(e) Describe procedures which the committee will follow to insure prompt reporting to the committee of proposed changes in the activity and of any unanticipated problems, involving risks to subjects or others and to insure that any such problems, including adverse reactions to biologicals, drugs, radioisotope labelled drugs, or to medical devices are promptly reported to DHEW.

(f) Indicate at what time intervals the committee will meet to provide for continuing review. Such review must occur no less than annually.

§ 46.8 Evaluation and disposition of assurances.

(a) All assurances submitted in accordance with §§ 46.6 and 46.7 shall be evaluated by the Secretary through such officers and employees of the DHEW and such experts or consultants engaged for this purpose as he determines to be appropriate. The Secretary's evaluation shall take into consideration, among other pertinent factors, the adequacy of the proposed committee in the light of the anticipated scope of the applicant organization's activities and the types of subject populations likely to be involved, the appropriateness of the proposed initial and continuing review procedures in the light of the probable risks, and the size and complexity of the organization.

(b) On the basis of his evaluation of an assurance pursuant to paragraph (a) of this section, the Secretary shall (1) approve, (2) enter into negotiations to develop a more satisfactory assurance, or (3) disapprove. With respect to approved assurances, the Secretary may determine the period during which any particular assurance or class of assurances shall remain effective or otherwise condition or restrict his approval. With respect to negotiations, the Secretary may, pending completion of negotiations for a general assurance, require an organization otherwise eligible for such an assurance, to submit special assurances.

§ 46.9 Obligation to obtain informed consent; prohibition of exculpatory clauses.

Any organization proposing to place any subject at risk is obligated to obtain and document legally effective informed consent. No such informed consent, oral or written, obtained under an assurance provided pursuant to this part shall include any exculpatory language through which the subject is made to waive, or to appear to waive, any of his legal rights, including any release of the organization or its agents from liability for negligence.

§ 46.10 Documentation of informed consent.

The actual procedure utilized in obtaining legally effective informed consent and the basis for committee determinations that the procedures are adequate and appropriate shall be fully documented. The documentation of consent will employ one of the following three forms:

(a) Provision of a written consent document embodying all of the basic elements of informed consent. This may be read to the subject or to his legally authorized representative, but in any event he or his legally authorized representative must be given adequate opportunity to read it. This document is to be signed by the subject or his legally authorized representative. Sample copies of the consent form as approved by the committee are to be retained in its records.

(b) Provision of a "short form" written consent document indicating that the basic elements of informed consent have been presented orally to the subject or his legally authorized representative. Written summaries of what is to be said to the patient are to be approved by the committee. The short form is to be signed by the subject or his legally authorized representative and by an auditor witness to the oral presentation and to the subject's signature. A copy of the approved summary, annotated to show any additions, is to be signed by the persons officially obtaining the consent and by the auditor witness. Sample copies of the consent form and of the summaries as approved by the committee are to be retained in its records.

(c) Modification of either of the primary procedures outlined in paragraphs (a) and (b) of this section. Granting of permission to use modified procedures imposes additional responsibility upon the review committee and the organization to establish: (1) that the risk to any subject is minimal, (2) that use of

either of the primary procedures for obtaining informed consent would surely invalidate objectives of considerable immediate importance, and (3) that any reasonable alternative means for attaining these objectives would be less advantageous to the subjects. The committee's reasons for permitting the use of modified procedures must be individually and specifically documented in the minutes and in reports of committee actions to the files of the organization. All such modifications should be regularly reconsidered as a function of continuing review and as required for annual review, with documentation of reaffirmation, revision, or discontinuation, as appropriate.

§ 46.11 Certification, general assurances.

(a) *Timely review.* Unless the Secretary otherwise provides, all proposals involving human subjects submitted by organizations having approved general assurances must be given review and, when found to involve subject at risk, approval, prior to submission to DHEW. In the event the Secretary provides for the performance of organizational review of a proposal after its submission to DHEW, processing of such proposal by DHEW will under no circumstances be completed until such organizational review and approval has been certified. Unless the organization determines that human subjects are not involved, the proposal or application should be appropriately certified in the spaces provided on forms, or one of the following certifications, as appropriate, should be typed on the lower or right hand margin of the page bearing the name of an official authorized to sign or execute applications or proposals for the organization.

Human Subjects: Reviewed, Not at Risk, _____
(date)

Human Subjects: Reviewed, At Risk, Approved_____.
(date)

(b) *Proposals not certified.* Proposals not properly certified, or submitted as not involving human subjects and found by the operating agency to involve human subjects, will be returned to the organization concerned.

§ 46.12 Certification, special assurances.

(a) An applicant organization not having on file with DHEW an approved general assurance must submit for each application or proposal involving human subjects a separate special assurance and certification of its review and approval.

(b) Such assurance and certification must be submitted within such time limit as the Secretary may specify. An assurance and certification prepared in accordance with this part and approved by DHEW shall be considered to have met the requirement for certification for the initial grant or contract period concerned. If the terms of the grant or contract recommend additional support periods, certification shall be provided by the organization with applications for continuation or renewal of support in the manner prescribed in § 46.11(a).

§ 46.13 Proposals lacking definite plans for involvement of human subjects.

Certain types of proposals are submitted with the knowledge that subjects are to be involved within the support period, but definite plans for this involvement would not normally be set forth in the proposal. These include such activities as (a) institutional type grants where selection of projects is the responsibility of the institution, (b) training grants where training projects remain to be selected, and (c) research, pilot, or developmental studies in which involvement depends upon such things as the completion of instruments, or of prior animal studies, or upon the purification of compounds. Such proposals shall be reviewed and certified in the same manner as more definitive proposals. The initial certification indicates organizational approval of the applications as submitted, and commits the organization to later review of the plans when completed. Such later review and certification to the DHEW should be completed prior to the beginning of the budget period during which actual involvement of human subjects is to begin. Review and certification to the DHEW must in any event be completed prior to involvement of human subjects.

§ 46.14 Proposals submitted with the intent of not involving human subjects.

If a proposal does not anticipate involving or intend to involve human subjects, no certification should be included with the initial submission of the proposal. In those instances, however, when later it becomes appropriate to use all or part of awarded funds for one or more activities which will involve subjects,

each such activity shall be reviewed and approved in accordance with the assurance of the organization prior to the involvement of subjects. In addition, no such activity shall be undertaken until the organization has submitted to DHEW: (a) a certification that the activity has been reviewed and approved in accordance with this part, and (b) a detailed description of the proposed activity (including any protocol or similar document). Also, where support is provided by project grants or contracts, subjects shall not be involved prior to certification and organizational receipt of DHEW approval and, in the case of contracts, prior to negotiation and approval of an amended contract description of work.

§ 46.15 Evaluation and disposition of proposals.

(a) Notwithstanding any prior review, approval, and certification by the organization, all grant and contract proposals involving human subjects at risk submitted to the DHEW shall be evaluated by the Secretary for compliance with this part through such officers and employees of the Department and such experts or consultants engaged for this purpose as he determines to be appropriate. This evaluation may take into account, among other pertinent factors ,the apparent risks to the subjects, the adequacy of protection against these risks, the potential benefits of the activity to the subjects and to others, and the importance of the knowledge to be gained.

(b) Disposition. On the basis of his evaluation of an application pursuant to paragraph (a) of this section and subject to such approval or recommendation by or consultation with appropriate councils, committees, or other bodies as may be required by law, the Secretary shall (1) approve, (2) defer for further evaluation, or (3) disapprove support of the proposed activity in whole or in part. With respect to any approved grant or contract, the Secretary may impose conditions, including restrictions on the use of certain procedures, or certain subject groups, or requiring use of specified safeguards or informed consent procedures when in his judgment such conditions are necessary for the protection of human subjects.

§ 46.16 Cooperative activities.

Cooperative activities are those which involve organizations in addition to the grantee or prime contractor (such as a contractor under a grantee or a subcontractor under a prime contractor). If, in such instances, the grantee or prime contractor obtains access to all or some of the subjects involved through one or more cooperating organizations, the basic DHEW policy applies and the grantee or prime contractor remains responsible for safeguarding the rights and welfare of the subjects.

(a) *Organization with approved general assurance.* Initial and continuing review by the organization may be carried out by one or a combination of procedures:

(1) Cooperating organization with approved general assurance. When the cooperating organization has on file with DHEW an approved general assurance, the grantee or contractor may, in addition to its own review, request the cooperating organization to conduct an independent review and to report its recommendations on those aspects of the activity that concern individuals for whom the cooperating organization has responsibility under its own assurance to the grantee's or contractor's committee. The grantee or contractor may, at its discretion, concur with or further restrict the recommendations of the cooperating organization. It is the responsibility of the grantee or contractor to maintain communication with the committees of the cooperating organizaion. However, the cooperating organization shall promptly notify the grantee or contracting organization whenever the cooperating organization finds the conduct of the project or activity within its purview unsatisfactory.

(2) Cooperating organization with no approved general assurance. When the cooperating organization does not have an approved general assurance on file with DHEW, the DHEW may require the submission of a general or special assurance which, if approved, will permit the grantee or contractor to follow the procedure outlined in the preceding subparagraph.

(3) Interorganizational joint review. The grantee or contracting organization may wish to develop an agreement with cooperating organizations to provide for a review committee with representatives from cooperating organizations. Representatives of cooperating organizations may be appointed as ad hoc members of the grantee or contracting organization's existing review committee or, if cooperation is on a frequent or continuing basis as between a medical school and a group of affiliated hospitals, appointments for extended periods may be

made. All such cooperative arrangements must be approved by DHEW as part of a general assurance, or as an amendment to a general assurance.

(b) *Organizations with special assurances.* While responsibility for initial and continuing review necessarily lies with the grantee or contracting organization, DHEW may also require approved assurances from those cooperating organizations having immediate responsibility for subjects.

If the cooperating organization has on file with DHEW an approved general assurance, the grantee or contractor shall request the cooperating organization to conduct its own independent review of those aspects of the project or activity which will involve human subjects for which it has responsibility. Such a request shall be in writing and should provide for direct notification of the grantee's or contractor's committee in the event that the cooperating organization's committee finds the conduct of the activity to be unsatisfactory. If the cooperating organization does not have an approved general assurance on file with DHEW, it must submit to DHEW a general or special assurance which is determined by DHEW to comply with the provisions of this part.

§ 46.17 Investigational new drug 30-day delay requirement.

Where an organization is required to prepare or to submit a certification under §§ 46.11, 46.12, 46.13, or 46.14 and the proposal involves an investigational new drug within the meaning of The Food, Drug, and Cosmetic Act, the drug shall be identified in the certification together with a statement that the 30-day delay required by 21 CFR 130.3(a) (2) has elapsed and the Food and Drug Administration has not, prior to expiration of such 30-day interval, requested that the sponsor continue to withhold or to restrict use of the drug in human subjects; or that the Food and Drug Administration has waived the 30-day delay requirement; provided, however, that in those cases in which the 30-day delay interval has neither expired nor been waived, a statement shall be forwarded to DHEW upon such expiration or upon receipt of a waiver. No certification shall be considered acceptable until such statement has been received.

§ 46.18 Organization's executive responsibility.

Specific executive functions to be conducted by the organization include policy development and promulgation and continuing indoctrination of personnel. Appropriate administrative assistance and support shall be provided for the committee's functions. Implementation of the committee's recommendations through appropriate administrative action and followup is a condition of DHEW approval of an assurance. Committee approvals, favorable actions, and recommendations are subject to review and to disapproval or further restriction by the organization officials. Committee disapprovals, restrictions, or conditions cannot be rescinded or removed except by action of a committee described in the assurance approved by DHEW.

§ 46.19 Organization's records; confidentiality.

(a) Copies of all documents presented or required for initial and continuing review by the organization's review committee, such as committee minutes, records of subjects's consent, transmittals on actions, instructions, and conditions resulting from committee deliberations addressed to the activity director, are to be retained by the organization, subject to the terms and conditions of grant and contract awards.

(b) Except as otherwise provided by law information in the records or possession of an organization acquired in connection with an activity covered by this part, which information refers to or can be identified with a particular subject may not be disclosed except:

(1) with the consent of the subject or his legally authorized representative or;

(2) as may be necessary for the Secretary to carry out his responsibilities under this part.

§ 46.20 Reports.

Each organization with an approved assurance shall provide the Secretary with such reports and other information as the Secretary may from time to time prescribe.

§ 46.21 Early termination of awards; evaluation of subsequent applications.

(a) If, in the judgment of the Secretary an organization has failed materially to comply with the terms of this policy with respect to a particular DHEW grant

or contract, he may require that said grant or contract be terminated or suspended in the manner prescribed in applicable grant or procurement regulations.

(b) In evaluating proposals or applications for support of activities covered by this part, the Secretary may take into account, in addition to all other eligibility requirements and program criteria, such factors as: (1) whether the offerer or applicant has been subject to a termination or suspension under paragraph (a) of this section, (2) whether the offerer or applicant or the person who would direct the scientific and technical aspects of an activity has in the judgment of the Secretary failed materially to discharge his, her, or its responsibility for the protection of the rights and welfare of subjects in his, her, or its care (whether or not DHEW funds were involved), and (3) whether, where past deficiencies have existed in discharging such responsibility, adequate steps have in the judgment of the Secretary been taken to eliminate these deficiencies.

§ 46.22 Conditions.

The Secretary may with respect to any grant or contract or any class of grants or contracts impose additional conditions prior to or at the time of any award when in his judgment such conditions are necessary for the protection of human subjects.

[FR Doc. 74–12269 Filed 5–29–74; 8:45 am]

U.S. SENATE,
COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C., July 10, 1974.

Dr. J. R. NEWBROUGH,
Center for Community Studies, George Peabody College,
Nashville, Tenn.

DEAR DR. NEWBROUGH: Thank you for your letter of July 2, 1974 containing your views on record systems and registries for children. The information will be most helpful in our development of privacy legislation.

Hearings have been conducted, but I shall include your letter and enclosure in the printed record.

Enclosed are reprints describing the Committee investigation. As you will see, S. 3418 would apply to federal, state, local and private record-keeping while S. 3633 would cover federal, intergovernmental and other information systems receiving federal support. If, after reviewing the text of S. 3418 contained in the May 2nd Congressional Record excerpt, you wish to offer further comments, the Committee would welcome your expert advice.

With all kind wishes, I am

Sincerely yours,

SAM J. ERVIN, JR., *Chairman.*

CENTER FOR COMMUNITY STUDIES,
Nashville, Tenn., July 2, 1974.

Hon. SAM ERVIN,
Senator from North Carolina,
Senate Office Building, Washington, D.C.

DEAR SENATOR ERVIN: I notice from the newspapers that you are currently holding hearings on the matter of records systems. I have been particularly interested in them and wished to share two ideas about safeguards that I have developed. The background for these was a project on the Classification of Exceptional Children directed by Dr. Nicholas Hobbs, Provost, Vanderbilt University, Nashville, Tennessee. I prepared a memorandum to Dr. Hobbs (which I attach for your information) on the matter of Records Systems and Registries for children. The two final recommendations, however, are appropriate for all citizens. They are:

1. *Recommendation for registers and name-linked systems.* In order to protect the person, the contents of the information held in the computer or linkage system should be periodically (yearly) printed out and provided to the person in complete detail. The system should also record the name, agency, date and content of information shared for each time the person's file is accessed and information removed.

2. *General recommendation.* All information should be reviewed by the person and the agency, institution or system each ten years (keyed to the person's

dicennial birthdays). Any information to be retained must have the joint agreement of the person and the agency. All other information is to be destroyed.

If I may provide further information, I should be happy to do so.

Sincerely,

J. R. NEWBROUGH.

CENTER FOR COMMUNITY STUDIES,
Nashville, Tenn., November 28, 1973.

MEMORANDUM

To: Nicholas Hobbs.
From: J. R. Newbrough.
Date: November 28, 1973.
Subject: Section for Final Report on Records and Registries.

I. I based the following on your section, Lister's paper, the sources cited in the draft, and some of my own thoughts. It is now in *First draft* form for your, the staff's, and Bert Brim's review. Would you collect the replies and suggestions for alteration? If you want, I will then work it over again.

II. *Records and Record-keeping.*—Records are kept on all children as part of their contacts with service organizations. The schools maintain a cumulative student record that serves as a dossier. The exceptional child is particularly exposed to the risks of record-keeping since the characteristics which prompt the institution to help or to control also lead them to create and retain records (Baker, Lister, & Milhous, 1973).

Three problems are contained in the record-keeping matter which represents threats to the civil liberties of the child:

(1) *Privacy.*—This involves the collection of information not actually needed for service purposes. This same information may become information which limits opportunities of the child in the future.

(2) *Confidentiality.*—This involves the protection of information so that only those with a need and a right to know can have access to the information.

(3) *Due process.*—This refers to the extent to which the record content, sharing and interpretation is visible to the person and is subject, at least in part, to his or her control.

Record-keeping serves an archival and a communication function in institutions. The records are a by-product of the service and are often handled by staff not in direct service work. Specialists (librarians or clerks) manage the records as if they were impersonal information collections (like books). Procedures to protect confidentiality and to provide due process represent complicating aspects of the procedure which requires more procedures and rules and manpower. Further, the professional or the agency regards the record as his property, to be managed as seen appropriate for their professional purposes. The individual person is then in no position to protect his own interests.

In addition to these institutional practices which present threats to individual civil liberties, there is the status of the child legally and socially that complicates the picture, particularly as regards due process (taken from Baker, Lister, & Milhous, 1973).

(1.) The child is not regarded as a full-member of society with the same rights as a citizen.

(2.) Whatever rights the child is understood to have is nearly always exercised through the child's parents.

(3.) With no citizens' rights of privacy and confidentiality clear under existing law, the exceptional child is often in a special status created by the view of him as an inferior child.

These three aspects make it difficult for there to be proper safeguards established for exceptional children, or children in general. And were they established, the procedures necessary to ensure that the parents were acting in the best interests of (or as an agent for) the child would represent a major challenge.

Recommendation for agencies and institutions. In order to insure responsible and ethical practices in record-keeping, each agency establish a Records Policy Board composed of appropriate professional people, of legal counsel on civil rights matters and of parents or their representatives. The Records Policy Board would:

(1) develop guidelines and procedures for record-keeping,[1]
(2) monitor and review procedures,
(3) take decisions to disseminate information outside the agency in instances where prior consent of the parents was not possible or feasible,
(4) hear complaints,
(5) impose sanctions for the misuse of records.

Recommendation on due process.—In order for parents to serve as an informed caretaker of the child and to provide for their ability to protect the privacy and confidentiality of the child, the following procedures should be adopted by professional societies, service agencies and institutions. Where these fail, parents' organizations should take action to get them enacted into state law.

(1) Parents and legal representatives of "exceptional" children should be given periodic notice of the information collected and maintained about such children, the purposes for which it is maintained, its uses, the period for which it will be retained, and the persons or agencies to whom it is available.

(2) Parents and legal representatives of "exceptional" children should be given access on reasonable terms to records maintained about their children. Records should be withheld from them only under the authorization of the relevant Records Policy Board.

(3) Parents and legal representatives of "exceptional" children should be afforded reasonable opportunities to contest the accuracy or completeness of records maintained about their children.

(4) An agency that would work to protect the interests of the child should be established in each community. This agency would serve as a third party in contests over contents of records, and objections to dissemination and misuse of information.

III. *Registers and the tracking of handicapped children.*—Registration as a process of collecting information on cases of disorders and handicaps is fairly widespread in the health field, and has been generally accepted for the social security system. In the social service delivery field, there was a concern in the 1920's about individuals and families who used more than one agency for service and who appeared to be getting more than their "fair share" of the services resources. In recent years, psychiatric case registers became a popular way of centralizing information on the total picture of service delivery (Baldwin, 1970). Those which were established in Monroe County, New York, and the state of Maryland have continued since the early 1960's and are still being used. Several were also established in Britain.

Registers particular to children are a new development and are being developed under a variety of auspices. Two examples are the Migrant Student Record Transfer System (State Department of Education, Little Rock, Arkansas) and the Maryland Data System for the Handicapped (State Department of Education, Baltimore, Maryland).

The Migrant Student Record Transfer System (MSRTS) was established to allow school systems to maintain central records on migrant school children and to have access to the information as the child moves from school to school (Miller, 1971). It has been made technically functional with some procedural ways of limiting access to the information (Braswell, personal communication). Confidentiality and access remains a major problem since project policies are the major policies which govern the information use, and can be changed or breached by the application of force. Legal protections would seem to be lacking.

The Maryland Data System for the Handicapped (MDSH) began for the purpose of getting unduplicated counts of handicapped children so that state resources could be made available to the needs. Identity was needed for the input of information; output was grouped so that identities were lost. This allowed the MDSH staff to limit access to the identifying information to the agency

---

[1] As sources for guidelines it is recommended that Boards consult the following:

Goslin, D. A. (Chairman) *Guidelines for the collection, maintenance and dissemination of pupil records.* (Report of a conference on the ethical and legal aspects of school record-keeping, 1969). New York: Russell Sage, 1970.

U.S. Department of Health, Education, and Welfare. *Records, computers and the rights of citizens.* (Report of the Secretary's Advisory Committee on Automated Personal Data Systems, DHEW Publication No. (05)73-94). Washington, D.C.: U.S. Government Printing Office, 1973.

Wheller, S. (Ed.) *On record: Files and dossiers in American life.* New York: Russell Sage, 1969. (See especially the Goslin and Bardier chapter.)

Miller, A. R. *The assault on privacy: Computers, data banks and dossiers.* Ann Arbor: The University of Michigan Press, 1971.

Westin, A. F. *Privacy and freedom.* New York: Atheneum, 1967.

offered it in the first place. The director noted that they are quite concerned about the labels currently in use and have established a working committee of cooperating agencies and interested professionals to help evolve them to more functional behavioral and educational forms.

Recommendation for registers and name-linked systems. In order to protect the person, the contents of the information held in the computer linkage system should be periodically (yearly) printed out and provided to the person in complete detail. The system should also record the name, agency, date and content of information shared for each time the person's file is accessed and information removed.

General recommendation. All information should be reviewed by the person and the agency, institution or system each ten years (keyed to the person's decennial birthdays). Any information to be retained must have the joint agreement of the person and the agency. All other information is to be destroyed.

MEDICAL RECORDS

Ethical Aspects of Medical Confidentiality

(By LeRoy Walters, Ph. D., Director, Center for Bioethics, Kennedy Institute, Georgetown University, Washington, D.C., presented at the Sixth Buffalo Conference on Computers in Clinical Medicine, Niagara Falls, N.Y., June 19, 1974)

This paper will be divided into four parts. In the first part, we shall briefly survey the history of the principle of medical confidentiality. In Part II we will examine the philosophical justification of the principle. The third part of the paper will explore possible grounds for violating the principle of confidentiality. In the final part of the paper we will turn specifically to the problem of confidentiality in computerized health-data systems.

I. The Principle of Medical Confidentiality: Historical Sketch

In this section we shall survey how two traditions have treated the principle of medical confidentiality, the *ethical* tradition and the *legal* tradition.

Within the ethical tradition the most extensive and detailed references to the principle of medical confidentiality occur within codes of professional ethics. The ancient works of Hindu medicine mention the obligation of medical secrecy.[1] For the Western tradition of medical ethics, however, the fundamental statement concerning medical confidentiality occurs in the Hippocratic Oath. There we read:

> What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.[2]

This affirmation of the principle of confidentiality in the Hippocratic Oath exerted a strong influence on the formulation of subsequent codes of medical ethics. The principle recurs in the first great modern textbook of professional ethics for physicians, Thomas Percival's *Medical Ethics*, published in 1803. Percival noted:

> Secrecy and delicacy, when required by peculiar circumstances, should be strictly observed. And the familiar and confidential intercourse, to which the faculty are admitted in their professional visits, should be used with discretion and with the most scrupulous regard to fidelity and honour.[3]

Percival's statement was reproduced practically verbatim in the first major American code, *The Code of Medical Ethics*, adopted by the American Medical Association in 1847.[4]

In more recent times the principle of medical confidentiality has been reaffirmed in numerous codes of professional ethics. The International Code of Medical Ethics adopted by the World Medical Association contains a strong statement of the principle:

> A doctor owes to his patient absolute secrecy on all which has been confided to him or which he knows because of the confidence entrusted in him.[5]

---

[1] See the English translation of the *Charaka Samhita* in M. B. Etziony, *The Physician's Creed* (Springfield, Ill.: Charles C. Thomas, 1973), pp. 15–17.

[2] Translated in Ludwig Edelstein, "The Hippocratic Oath: Text, Translation and Interpretation" in Owsei Temkin and C. Lilian Temkin, eds., *Ancient Medicine: Selected Papers of Ludwig Edelstein* (Baltimore: Johns Hopkins University Press, 1967), p. 6.

[3] Thomas Percival, *Medical Ethics*, edited by Chauncey D. Leake (Baltimore: Williams & Wilkins, 1927), p. 90.

[4] American Medical Association, *Code of Medical Ethics* (New York: H. Ludwig & Co., 1848), p. 13.

[5] Quoted by Etziony, *Physician's Creed*, p. 88.

The most recent version of the AMA's "Principles of Medical Ethics" devotes a separate section to the topic of medical confidentiality.[6]

In addition to appearing in codes of professional ethics for *physicians*, the principle of confidentiality also plays a prominent role in the ethical codes of various allied-health personnel, including nurses, medical social workers, and medical record librarians.[7] Of particular interest to our topic of today is a statement in the Code of Ethics of the American Association of Medical Record Librarians:

> As a member of one of the paramedical professions [the librarian] shall: . . .
>
> (2) Preserve and protect the medical records in his custody and hold inviolate the privileged contents of the records and any other information of a confidential nature obtained in his official capacity, taking due account of applicable status and of regulations and policies of his employer.[8]

Professional codes of ethics have been the main locus of ethical discussion concerning the principle of medical confidentiality. However, there are two other non-legal sources which should at least be mentioned in passing. The first is the tradition of Western religious ethics. The literature of various religious groups, particularly Jews and Roman Catholics, has devoted substantial attention to questions of medical ethics.[9] On the specific issue of medical confidentiality Jewish religious ethics is totally silent.[10] In contrast, Catholic textbooks of moral theology have devoted substantial attention to the question of medical confidentiality, perhaps in part because of its obvious parallels with the confidential relationship of priest and penitent.[11] Within the moral-theology textbooks are extended discussions of the nature of a secret, mental reservation, and the circumstances under which professional secrets may or may not be revealed.[12]

The other major non-professional source of ethical discussion concerning medical confidentiality is the emergent patient's-rights movement. Probably the most important document resulting from pressures generated by the movement is the "Patient's Bill of Rights," published by the American Hospital Association in 1972. In that document one reads:

> 6. The patient has the right to expect that all communications and records pertaining to his care should be treated as confidential.[13]

The *legal* tradition has also wrestled at length with the problem of medical confidentiality. In many cases, the law has simultaneously discussed the analogous questions of confidential communications between attorneys and clients and between ministers or rabbis and persons who solicit their advice.

Two kinds of legal protection for medical confidentialty can be distinguished: positive protection and negative protection. Positive protection refers to legal sanctions which can be applied against physicians who reveal confidential information about their patients. In English and American law the patient injured by such a breach can seek a remedy at law by bringing suit. In contrast, on the European continent the violation of medical secrecy by the physician is punishable or punished according to provisions of the crminal law.[14]

Negative protection of medical confidentiality is provided by laws which establish communications between physician and patient as privileged communications and which thereby exempt the physician from the normal obligation to testify before a court of law. The English Common Law did not consider as

---

[6] American Medical Association, Judicial Council, *Opinions and Reports* (Chicago: American Medical Association, 1968), p. VII.

[7] See Etziony, *Physician's Creed*, pp. 120–122, 127–128, 135–137.

[8] *Ibid.*, p. 136.

[9] For a survey of the professional and religious sources of medical ethics see LeRoy Walters, "Medical Ethics," in the Supplement to *The New Catholic Encyclopedia* (New York: McGraw-Hill, forthcoming). Two standard textbooks of religious thought concerning medical ethics are Immanuel Jakobovits, *Jewish Medical Ethics* (New York: Bloch Publishing Company, 1959) and Charles J. McFadden, *Medical Ethics* (6th ed.; Philadelphia: F. A. Davis Co., 1967).

[10] Jakobovits, *Jewish Medical Ethics*, p. 210.

[11] On this point see Ralph Slovenko, *Psychiatry and Law* (Boston: Little, Brown and Company, 1973), p. 435. Within Catholic moral theology textbooks, discussion of medical confidentiality usually appears at one of three points: in the treatment of the Eighth Commandment (vs. lying) or of justice and right (*de justitia et jure*), or in the consideration of special duties which attach to particular professions or states in life (Robert E. Regan, *Professional Secrecy in the Light of Moral Principles: with an Application to Several Important Professions*). (Washington, D.C.: Augustinian Press, 1943), p. 124.

[12] See Regan's comprehensive survey in *Professional Secrecy*, pp. 114–148.

[13] American Hospital Association, "Patient's Bill of Rights" (Chicago: American Hospital Association, 1972).

[14] Regan, *Professional Secrecy*, p. 119.

privileged the communications which pass between physicians and patients. Since the common law has formed the basis for American jurisprudence, it was to be expected that early American law would also lack any provision protecting communication between physicians and patients. However, in 1828 New York state by statute made physician-patient communication privileged. The New York statute, which became the model for similar statutes adopted in many other states of the Union, read as follows:

> No person duly authorized to practice physic or surgery shall be allowed to disclose any information which he may have acquired in attending any patient, in a professional character, and which information was necessary to enable him to prescribe for such patient as a physician, or to do any act for him as a surgeon.[15]

As of 1973, forty-three states and the District of Columbia had enacted general physician-patient privilege statutes. In addition, at least seventeen states have recently adopted laws which protect psychiatrist-patient or phychologist-client communications.[16]

II. THE PRINCIPLE OF MEDICAL CONFIDENTIALITY: PHILOSOPHICAL JUSTIFICATION

We turn now from history to philosophy, from the question of *when* and *how* the principle of medical confidentiality was formulated to the question of *why* is is important. There are, in my view, two primary philosophical arguments in favor of preserving medical confidentiality. The first argument is pragmatic and refers to possible long-term consequences. The second argument is non-pragmatic and speaks of respect for the rights of persons.

The pragmatic argument for the preservation of medical confidentiality is that without such confidentiality the physician-patient relationship would be seriously impaired. More specifically, the promise of confidentiality encourages the patient to make a full disclosure of his symptoms and their causes, without fearing that an embarrassing condition will become public knowledge.[17]

Among medical professionals, psychotherapists have been particularly concerned to protect the confidentiality of their relationship wtih patients. In the words of one psychiatrist,

> The patient in analysis must learn to free associate and to break down resistances to deal with unconscious threatening thoughts and feelings. To revoke secrecy after encouraging such risk-taking is to threaten all future interaction.[18]

A second argument for the principle of medical confidentiality is that the right to a sphere of privacy is a basic human right. In what is perhaps the classic essay concerning the right of privacy, Samuel Warren and Louis Brandeis wrote in 1890 that the common law secured "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." [19] Present-day spokesmen for the right of privacy frequently employ the imagery of concentric circles or spheres. In the center is the "core self," which shelters the individual's "ultimate secrets"—"those hopes, fears, and prayers that are beyond sharing with anyone unless

---

[15] New York Revised Statutes, 1828, II, 406, Part III, c. vii, art. 8, paragraph 3; quoted by Elyce Zenoff, "Confidential and Privileged Communications" *Journal of the American Medical Association* 182 (6): 657, 10 November 1962. For a comprehensive discussion of the physician-patient privilege see Clinton DeWitt, *Privileged Communications Between Physician and Patient* (Springfield, Ill.: Charles C. Thomas, 1958).

[16] Dennis Helfman, *et al.*, "Access to Medical Records" in the *Appendix* to U.S., Department of Health, Education and Welfare, *Report of the Secretary's Commission on Medical Malpractice* (Washington, D.C.: U.S. Government Printing Office, 1973), pp. 178–179. The authors of this report note that in the 1971 draft of the Proposed Federal Rules of Evidence the physician-patient privilege is abolished but a psychotherapist-patient privilege is retained (*ibid.*, p. 182).

[17] A similar line of argument was advanced in favor of testimonial privilege for physicians in *Randa* v. *Bear*, 50 Wash. 2d 415, 312 P. 2d 640 (1957); cited by William J. Curran and E. Donald Shapiro, *Law, Medicine, and Forensic Science* (2nd ed.; Boston: Little, Brown and Company, 1970), p. 377.

[18] Harvey L. Ruben and Diane D. Ruben, "Confidentiality and Privileged Communications: The Psychotherapeutic Relationship Revisited," *Medical Annals of the District of Columbia* 41(6): 365, June 1972.

[19] The Warren-Brandeis article appeared in the *Harvard Law Review*, vol. 4, 1890, at p. 193. This quotation is taken from Susan Beggs-Baker, *et al.*, "Individual Privacy Considerations for Computerized Health Information Systems," *Medical Care* 12(1): 79, January 1974. For a perceptive recent treatment of the right to privacy see Charles Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge, Mass.: Harvard University Press, 1970), chap. 9. The constitutional right of privacy has recently been affirmed by the U.S. Supreme Court in the cases *Griswold* v. *Connecticut* (381 U.S. 479, 85 S. Ct. 1678 (1965)] and *Katz* v. *United States* [389 U.S. 347, 88 S. Ct. 507 (1967)].

the individual comes under such stress that he must pour out these ultimate secrets to secure emotional release."[20] According to this image, the next largest circle contains intimate secrets which can be shared with close relatives or confessors of various kinds. Successively larger circles are open to intimate friends, to casual acquaintances, and finally to all observers.

The principle of medical confidentiality can be based squarely on this general right of privacy. The patient, in distress, shares with the physician detailed information concerning problems of body or mind. To employ the imagery of concentric circles, the patient admits the physician to an inner circle. If the physician, in turn, were to make public the information imparted by the patient—that is, if he were to invite scores or thousands of other persons into the same inner circle—we would be justified in charging that he had violated the patient's right of privacy and that he had shown disrespect to him as a human being.

These two arguments for the principle of medical confidentiality—the argument based on probable consequences of violation and the argument based on the right of privacy—seem to constitute a rather strong case for the principle. However, we have not yet faced the question whether the principle of confidentiality is a moral absolute or whether it can be overridden by other considerations. To that subject we now turn.

III. THE PRINCIPLE OF CONFIDENTIALITY: POSSIBLE GROUNDS FOR VIOLATING THE PRINCIPLE

There are, in my view, three general reasons which might conceivably justify violating the principle of confidentiality.[21] The first is that the principle may come into conflict with the rights of the patient himself.

To illustrate, one can envision a situation in which a patient, in a temporary fit of depression, threatens to kill himself or to perform an irrational act which will almost certainly destroy his own reputation. In the case of threatened suicide one finds oneself weighing a secret vs. a life. Perhaps the physician should feel free, in such a case, to violate the principle of confidentiality and to involve a third party for the protection of the patient himself.

A second possible ground for violating the principle of confidentiality is that it may conflict with the right of an innocent third party. In older textbooks of moral theology, one can discover hypothetical cases constructed to illustrate this dilemma. Often the case involves a physician and a young couple about to be married. Because of his professional relationship with the husband-to-be, the physician knows that the man is concealing a condition of infective syphilis or permanent impotence from his future wife. The question then arises whether the physician should violate the principle of confidentiality in order to warn the unsuspecting innocent party.[22]

In our own time the physician's dilemma is more likely to concern the case of a "battered child." If the abused child is brought to the physician by the battering parents, the physician faces an immediate conflict of loyalties. Does he owe it to his adult patients to keep confidential the fact that they have abused the child. Or is he under obligation to protect the child from further harm by disclosing the child's injuries to the proper public authorities? It should perhaps be noted in passing that most states in the U.S. *require* that the physician report child-abuse cases to the appropriate governmental agency.

A third possible ground for violating the principle of confidentiality is a serious conflict between the principle and the rights of society in general. The possibility of such a conflict was formally recognized in 1912,[23] when the American Medical Association revised its code of ethics. A new clause was introduced into the confidentiality section of the code, specifically authorizing the physician to report communicable diseases, even if such reports were based on confidential information. The justification for this type of disclosure was, of course, the protection of society at large from the spread of infectious disease.[24]

At present, various states require reports of particular types of contagious disease. Almost universally, the physician is legally obligated to report cases of

---

[20] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 33.

[21] The following analysis parallels, in part, Regan's discussion of "various conflicts between the duty of medical secrecy and other rights and duties" (*Professional Secrecy*, pp. 138–148).

[22] This illustration is drawn from Regan, *Professional Secrecy*, pp. 143–147.

[23] Helfman, *et al.*, "Access to Medical Records," pp. 180–181.

[24] Regan, *Professional Secrecy*, p. 116. A similar, although more general, exception to the confidentiality-obligation is included in the current AMA "Principles of Medical Ethics" (Judicial Council, *Opinions and Reports*, p. VII).

venereal disease to the proper governmental authorities. The reporting of tuberculosis is also frequently required. State provisions for protecting the confidentiality of such public-health reports vary widely with about half of the states taking measures to prevent public disclosure of the data.[25] Whenever states require physicians to report such data concerning communicable diseases, the general justification for the violation of physician-patient confidentiality is that society at large must be protected.

There is a second type of situation in which the principle of confidentiality and the public good seem to come into sharp conflict. In these cases the physician discovers a serious medical problem in a patient whose occupation makes him responsible for the lives of many other persons. Two standard examples are a railroad signalman who is discovered to be subject to attacks of epilepsy, or an airline pilot with failing eyesight. A case reported in a recent essay on medical secrecy reads as follows:

> Last year 30 people were killed when a bus driver had a heart attack and plunged his bus into the East River in New York City. The driver's physician had known about the bad heart, had cautioned him not to drive, but felt he could not report it to the company since the patient might lose his job.[26]

In cases involving such critical occupations, some would argue that the physician's duty to protect the lives of many persons overrides his obligation to observe the principle of medical confidentiality.

In the future we are likely to see furious battles fought over the question of medical confidentiality vs. the public good. Let me cite three examples. Already one hears rhetoric which implies that genetic disorders are quasi-contagious diseases.[27] According to this viewpoint, members of future generations will be "infected" if decisive action is not taken now. Is it possible that such pressures will lead to the requirement that physicians routinely report genetic defects to public-health authorities? To cite a second example, epidemiologists vigorously pursue new correlations between chronic diseases and particular environmental factors or medical conditions. Their studies frequently require surveys of total populations or random samples of such populations.[28] Will the desire of patients to keep their medical records confidential and their refusal to take part in such epidemiological studies come to be seen as an antisocial act as a failure to perform a civic duty? Third, it is at least conceivable that the concept of public health could be expanded to include "economic contamination." According to this view, any disease which prevents a person from being a fully-productive member of the labor force would be seen as a hazard to the society's overall economic health, particularly if public funds were being used to defray the expenses of the illness. Cost-benefit analysis would indicate that because of the illness other persons in the society would need to work to subsidize the relatively-less-productive ill person. As one economist put it, well persons would become, at least partially, the "economic slaves" of the patient.[29] If the concept of public health is expended in this economic direction, it seems likely that there will be tremendous pressure directed against maintaining the medical confidentiality of patients whose treatment is subsidized by public funds.

My own view is that the physician has what moral philosophers call a prima facie obligation to preserve the principle of medical confidentiality.[30] This obligation is based on the two considerations mentioned in Part II above, a concern for protecting the physician-patient relationship and a desire to respect the patient's right of privacy. Thus, the burden of proof must be assumed by anyone who wishes to argue that the principle of medical confidentiality should be violated. However, there are, in my view, some cases in which this prima facie obligation can be overridden because of other very weighty considerations, for example, the desire

---

[25] Helfman, *et al.*, "Access to Medical Records," p. 181. State laws requiring that cases of drug addiction be reported would be justified by means of analogous arguments (*ibid.*).

[26] Henry A. Davidson, "Professional Secrecy," in E. Fuller Torrey, ed., *Ethical Issues in Medicine: the Role of the Physician in Today's Society* (Boston: Little, Brown and Company, 1968), p. 194.

[27] See, for example, Amitai Etzioni, *Genetic Fix* (New York: Macmillan, 1973), esp. chap. 4.

[28] Great Britain, Medical Research Council, "Responsibility in the Use of Medical Information for Research," *British Medical Journal* 1 (5847): 213–216, 27 January 1973.

[29] See the comments of the economist Lester Thurow on a related issue in Betty Cochran, "Conference Report: Conception, Coercion, and Control," *Hospital and Community Psychiatry* 25(5), 287, May 1974.

[30] William Frankena, *Ethics* (2nd ed., Englewood Cliffs, N.J.: Prentice-Hall, 1973), p. 26–28.

to protect the patient's own life or the lives of other persons. According to this view, then, the physician's duty to observe the principle of medical confidentiality is a very important moral obligation, but not an absolute obligation or one's only obligation.

IV. THE PRINCIPLE OF MEDICAL CONFIDENTIALITY AND COMPUTERIZED HEALTH-DATA SYSTEMS

In a sense, computers introduce only a quantitative change into the traditional physician-patient relationship. Thus, it would seem at first glance that no fundamentally new challenges to the principle of medical confidentiality are raised by the development of computerized health-data systems. Let me explain.

The increasing participation of subspecialists and allied health personnel in medical care has meant that an ever-widening circle of persons has access to the medical records of patients, particularly the records of hospital patients. We have noted that each new group with access has tended to develop a professional code which includes a pledge to preserve the confidentiality of the record. Automation does not fundamentally change this situation, provided that access is restricted to the same circle of persons. At most, the new situation would seem to require that the persons operating the computerized health-data system adopt a similar code of confidentiality.

Similarly, the gathering of the patient's disparate medical records into a single comprehensive file does not seem to raise qualitatively new problems, any more than a manual operation of photocopying, cutting, and pasting scattered records into a single master record would. So long as the rules of access to particular parts of the file remain the same, the medical-confidentiality issue remains fundamentally the same.

However, the *quantitative* difference is perhaps significant. Because of the efficiency of automated systems, violations of medical confidentiality may appear to be easier. Because of the amount of data which may be included in a comprehensive patient file, the damage to the patient whose confidentiality is violated may be proportionately greater.

In addition, the transition from manual to automated health-data systems provides us with an occasion to think through ethical issues which we should perhaps have confronted before this point but which we have largely ignored. I would like to mention three such issues.

The first is the issue of *patient access to his own confidential medical record.* As you know, this question has been the subject of considerable debate during the past two years.[31] In my view, the development of comprehensive health records in computerized health-data systems makes it more important than ever for the patient to have a way to correct misinformation in his file. I say this for two reasons. First, if lifetime records are compiled, information more than several years old may be badly outdated and therefore convey a false impression of the patient's current medical condition. Second, since many subspecialists do not know the patient personally, there is no built-in check against serious misinformation about the patient. The precise mechanism for patient access remains to be worked out. Majority opinion seems to favor access through an intermediary, perhaps a lawyer or an ombudsman.[32]

A second issue which merits thorough discussion is *the grading of confidential information according to different levels of sensitivity.* The effort to determine degrees of sensitivity is reminiscent of our earlier discussion of concentric circles of privacy. It is perhaps Sweden which has gone furthest in attempting to deal with the question of assessing the relative sensitivity of medical data. In the Stockholm district several hospitals are linked to a central data bank which stores all medical data on every patient. This information is graded for sensitivity into three categories; details are decided upon by a reference committee. The most sensitive grade of information includes data concerning psychiatric problems, venereal disease, and gynecological problems. Users of the system are assigned codes which provide access only to particular grades of confidential information.[33]

A final issue which I wish to raise is *the question of guaranteeing medical confidentiality.* Until now, the primary positive protection for patients against un-

[31] See U.S. Department of Health, Education, and Welfare, *Medical Malpractice: Report of the Secretary's Commission on Medical Malpractice,* pp. 75–77; and Budd N. Shenkin and David C. Warner, "Giving the Patient His Medical Record: a Proposal to Improve the System," *New England Journal of Medicine* 289(13): 688–692, 27 September 1973.

[32] U.S., Department of Health, Education, and Welfare, *Medical Malpractice,* p. 77.

[33] "Research and Confidentiality," *C.M.A. Journal* 108: 1351, 2 June 1973.

warranted disclosure of medical data has been the development of various codes of professional ethics. In effect, various professional groups have solemnly promised not to violate the principal of medical confidentiality. Professional self-regulation has been the primary sanction against abuse; legal remedies have been, except in cases of gross abuse, relatively unavailable. Now that more complete data files are being stored in automated systems, it is perhaps time to go beyond codes of ethics and to seek more precise legal guarantees for medical confidentiality. One scholar has proposed, for example, that the patient should be expressly protected by law against injuries resulting from a "breach of [medical] confidence." [34]

In summary, the principle of medical confidentiality has a long history. The primary arguments in favor of the principle are that it preserves the physician-patient relationship and that it expresses respect for the patient's right of privacy. I have sought to argue that the principle of medical confidentiality should be observed in most cases but that it may be violated when a higher value—for example, human life, would be threatened by observing it. And finally, we have noted that the development of computerized health-data systems brings into sharp relief a series of critical issues which urgently require our attention and discussion.

The planners of this symposium are to be commended for inviting us to reflect on these issues and for their pioneering efforts to develop institutional models for the protection of medical confidentiality.[35]

STATE OF NEW YORK,
LEGISLATURE OF ERIE COUNTY,
CLERK'S OFFICE,
Buffalo, N.Y., July 3, 1974.

TO WHOM IT MAY CONCERN:

I Hereby Certify, That at a Session of the Legislature of Erie County, held in the County Hall, in the City of Buffalo, on the second day of July A.D., 1974 a Resolution was adopted, of which the following is a true copy:

Whereas, computers have revolutionized information handling in business & Industry, and are being increasingly used for efficient collection of clinical information, and

Whereas, the risk of technological progress is often the loss of our privacy, with the danger of a "Big Brother" type of data collection and distribution, which practice if unrestrained may become uncontrollable, resulting in unrestricted inspection by employers, insurance companies, government agencies, etc., and

Whereas, we may reveal highly confidential information in a doctor's office which, while valuable for health treatment, should not be revealed indiscriminately, and

Whereas, our immediate hope of averting misuse of such information is to legislate tough rules governing use of computers and data banks, thereby affording genuine protection of privacy for citizens, and

Whereas, the Medical Society of the County of Erie has recognized this potential threat to privacy by creating a Joint Task Group on Confidentiality of Computerized Medical Records for the study of the moral, social, legal, medical, and technological aspects of computer storage of highly sensitive medical data, and

Whereas, the results of the study by the Task Force was a concept of dedicated "ethical health data centers" which would be obliged to upgrade medical care and be responsible for protecting privacy of all patients, which concept was endorsed by the House of Delegates of the Medical Society of the State of New York, and

Whereas, the Medical Privacy Act which calls for a federal administrator to approve plans of individual states which would allow for licensing and monitoring of data centers which sort and process medical data, is pending in Congress along with other proposals dealing with the subject,

Now, therefore, be it resolved, that the Erie County Legislature hereby endorses the concept set forth by the Medical Task Force, which has shown commendable

[34] Roedersheimer, "Action for Breach of Medical Secrecy Outside the Courtroom," *University of Cincinnati Law Review* 36 (1966), 103; cited by Helfman, *et al.*, "Access to Medical Records," p. 183.

[35] I wish to thank Ms. Doris M. Goldstein, Librarian to the Center for Bioethics, for her bibliographical assistance in the preparation of this essay.

concern for the patient's right to share in the basic decision of what personal information is to be revealed, and hereby endorses the Medical Privacy Act which will force states to assume legal responsibility and leadership, by devising procedures that would preserve the medical advantages of modern computer technology, while at the time protecting patient privacy, and be it further

Resolved, that certified copies of this resolution be sent to Dr. E. R. Gabrieli at E. J. Meyer Memorial Hospital, the Congressmen representing Western New York, Caspar W. Weinberger, Secretary of Health, Education and Welfare, and Senator Sam J. Ervin, Jr.

JAMES E. HENNISSY,
Clerk of the Legislature of Erie County.

1974 HOUSE OF DELEGATES

REFERENCE COMMITTEE E

Subject: Confidentiality: A Release of Privileged Medical Information to Credit Reporting Agency

Introduced by: District of Columbia Society of Internal Medicine

Whereas, many life insurance companies are using the facilities of the Retail Credit Corporation to obtain privileged medical information from physicians concerning their patients' histories, and

Whereas, the potential for misuse of this privileged and highly confidential information exists through collection, access to/or dissemination of such information to/or from any unauthorized source, thus violating the rights of the patients, be it therefore

Resolved, That the American Society of Internal Medicine advise its members not to honor requests for medical information from other than life insurance companies directly, upon specific written authorization from the patient, and not to supply information of a privileged or confidential nature to other than the Medical Directors of the authorized life insurance companies, and be it further resolved, That the American Society of Internal Medicine inform all life insurance companies of its opposition to the use of any third party organization to collect, assemble or have access to any such privileged medical information.

Previous Action: Board of Trustees 11/73 approved statement on *Confidentiality* Board of Trustees 2/74 amended statement on *Confidentiality* and voted to recommend its adoption to the 1974 House of Delegates. See Board of Trustees Report B HD 74.

Fiscal Note: Less than $100.

DRS. MILLER JOHNSON AND MAXWELL, P.C.
PHYSICIANS, DIPLOMATES OF THE AMERICAN BOARD OF INTERNAL MEDICINE,
EUGENE, OREG., *September 6, 1974.*

HON. MARK HATFIELD
Senate Office Building, Washington, D.C.

DEAR SENATOR HATFIELD: I read with considerable interest your September Newsletter in regard to the privacy legislation. This area has been of considerable concern to a number of us in the medical field, since we are often asked to give detailed medical information on patients to the Retail Credit Corporation. Patients will sign the blanket release of information, presuming the information will go from one doctor to the physician director of a life insurance company. They are not aware that this information can be used to determine credit ratings on them by other than medical insurance companies.

Attempts to point this out to our patients often result in either the insurance agent or the patient getting angry. Sometimes the anger is turned toward the physician, who they feel is just trying to delay doing the job that he was assigned to do.

I have enclosed a resolution adopted by the American Society of Internal Melicine at their last annual meeting. I hope this may be of some help to you.

It would seem to me that a legislation should be promoted that would prevent life insurance companies from selling or combining their medical information for the use of credit agencies. I do not, of course, object to the insurance com-

pany medical directors coordinating their information with other insurance company medical directors for purposes of determining risk for medical insurance. I do not think, however, that private medical information should be allowed as a determinant in financial credit ratings. I see no reason why commercial credit unions should be doing the job of gathering medical information of the directors of insurance companies.

I am sure that the appropriate committee of the Medical Society of Internal Medicine would be happy to provide you with any additional information on this area.

Thank you for your attention.

Sincerely,

HUGH B. JOHNSTON, M.D.

THE COMMONWEALTH OF MASSACHUSETTS,
EXECUTIVE DEPARTMENT, STATE HOUSE,
Boston, July 15, 1974.

Secretary CASPER W. WEINBERGER,
Department of Health, Education, and Welfare,
Washington, D.C.

DEAR SECRETARY WEINBERGER: A number of administrators of state agencies, as well as Mr. Russell E. O'Connell, Commissioner of Massachusetts Rehabilitation Commission, have brought to my attention their concern over a requirement of the Social and Rehabilitation Services Administration (SRSA) that persons applying for vocational rehabilitation must complete a "case service report," (RSA–000) replete with sensitive personal and financial information, identified by a client's social security number.

I share their concern that the use of social security number for identification threatens the confidentiality of individual client records and potentially compromises the value of rehabilitation services. Already a number of social service agencies in the Commonwealth have refused to refer clients for vocational rehabilitation because of this requirement. They are fearful that individuals, particularly those suffering from disabilities that have a social stigma attached, such as "drug addiction", or "alcoholism", will suffer a residual impairment to functioning if their previous condition is widely recorded and possibly accessible. The collection of such information in a centralized, national data bank linked to the Social Security Administration can be viewed only with alarm.

I realize that because of our commitment to protect personal privacy, the SRSA has already acted to delete client name and address data collection requirements. However, I submit that the protection of personal privacy will not be guaranteed until the required identification of client records by social security number is also dropped. I urge you to take immediate action to recind this requirement.

In the meantime, I am directing the Massachusetts Rehabilitation Commission to substitute their internal numerical system for federal reporting requirements. Further, I ask that appropriate federal action be taken to safeguard the confidentiality of those records already collected on Massachusetts citizens.

I have asked Mr. Russell E. O'Connell to meet with appropriate federal officials to implement this new policy. I believe that we can meet the needs of your department to collect pertinent statistical data necessary for planning and program monitoring without sacrificing personal privacy and the confindetiality of client records.

Sincerely,

FRANCIS W. SARGENT.

45 C.F.R. 300
MRC-R300

U.S. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE
Social and Rehabilitation Service
National Center for Social Statistics

Mass. Rehab. Commission

Agency Code_____*
Case Number_____

CASE SERVICE REPORT, FEDERAL-STATE PROGRAM OF VOCATIONAL REHABILITATION

PART 1 (TO BE RECORDED AT TIME OF FIRST REFERRAL)

A. Last Name | First Name | Initial

C. Referral Date_____ D. Referral Source_____*
E. Age____dob_____ F. Sex: 1 ☐ Male; 2 ☐ Female

B. Address: Street and Number

G. Disability as Reported (describe)

City | County | (Code*) | Zip Code

Code_____*

PART 2 (TO BE RECORDED AT COMPLETION OF REFERRAL PROCESS)

A. Soc. Sec. No._____
B. SSDI Status at Referral_____*
C. Race_____*
D. Date Referral Process Completed
_____
E. Months in Statuses 00-02_____
F. Spanish Surname: Yes ☐ 1; No ☐ 2
G. Outcome of Referral Process:
NOT ACCEPTED: Reason_____*
1 ☐ from (00); 2 ☐ from (02)
Client Referred to_____* or
Referral Not Appropriate ☐ 00

If closed from status 00, complete items 3.A. thru 3.C. If closed from status 02, complete items 2.H. thru 2.R. and items 3.A. thru 3.C.

G. Outcome of Referral Process (continued):
ACCEPTED FOR: 03 ☐ 6-mos. Est. Eval. (04); 04 ☐ 18-mos. Est. Eval. (06); 05 ☐ VR Services (10)

Complete items 2.H. thru 2.R. DO NOT COMPLETE ANY OF PART 3 AT THIS TIME.

H. Disabling Conditions (describe)
1. Major
Code_____*
2. Secondary
Code_____*

I. Previous Closure within 36 months:
No ☐ 1; Yes-Outcome: Rehab. ☐ 2; Not Rehab. ☐ 3
If Yes-Months Since Last Closure_____
J. Marital Status_____*
K. Number of Dependents_____
L. Total Number in Family_____
M. Highest Grade Completed_____
N. Work Status_____*
O. Weekly Earnings $_____
P. Total Monthly Family Income (including earnings)_____*
Q. Public Assistance: Type_____*; Mo. Amt. $_____; Time on P.A._____*
R. Primary Source of Support_____*

PART 3 (TO BE RECORDED AT TIME OF CLOSURE)

Federal Special Program Identification*

None	1F	AFR	MMS	MAW	PO	WIN	SEC. 4	SF		SUM
										////
000	001	002	004	010	020	040	100	200	400	

Cost of Case Services (Dollars)

1. All Services - Total
2. Rehabilitation Facilities - Total
3. Social Security Trust Funds - Total
4. Extended Evaluation - Total

Social Security Trust Funds Cases Only:
1. Social Security Claim Type_____*
If Claim Type Code 2,3, or 4, enter Wage Earner's:
Last Name | First Name | Initial
Social Security Number
2. Check (x) if Administrative † Costs only ☐
† Includes counseling, guidance, and placement

Date Ext. Eval. Completed (if applicable)_____
SSDI Status at Time of Closure_____*
Work Status_____*
Weekly Earnings $_____*
Public Assistance: Type_____*; Mo. Amt. $_____
Occupation (title)_____
Code_____*

J. Number of Months on Agency Rolls:
1. In Extended Evaluation (statuses 04 or 06)_____
2. From Acceptance to Closure (statuses 10-24)_____
3. In Training (status 18)_____
4. Ready for or in Employment (statuses 20-22)_____

K. Outcome of Extended Evaluation or VR Services:
1 ☐ Closed from Ext. Eval. (status 08): Reason_____*
2 ☐ Closed Rehabilitated (status 26)
3 ☐ Closed Not Rehabilitated (status 28): Reason_____*
4 ☐ Closed Not Rehabilitated (status 30): Reason_____*

L. Services Provided: Indicate (x) if applicable

	Type of Service Provided or Arranged for by Agency	With Cost Only (1)	Without Cost Only (2)	With & Without Cost (3)
10	Diagnostic and Evaluation			
11	Restoration (Physical or Mental)			
12	TRAINING: College or University			
13	TRAINING: Other Academic (Elem. or HS)			
14	TRAINING: Business School or College			
15	TRAINING: Vocational School			
16	TRAINING: On-the-Job			
17	TRAINING: Personal & Voc. Adjustment			
18	TRAINING: Miscellaneous			
19	Maintenance			
20	Other Services			
21	Services to other family members			

M. State Agency Special Program Identification*

None										SUM
										////
000	001	002	004	010	020	040	100	200	400	

* These items are to be coded.

NCSS COPY

District Code | Date of Report | Counselor Signature and Code

FEBRUARY 15, 1974.

RUSSELL E. O'CONNELL,
Commissioner, Massachusetts Rehabilitation Commission,
Boston, Mass.

DEAR RUSS: This is in response to your letter regarding the data link between RSA and the Social Security Administration (SSA).

RSA has submitted Fiscal Year 1971 RSA–300 closure records to SSA and expects to receive tabulations within the next few months showing Calendar Year 1972 earnings from SSA records, of former VR clients and also earnings in the calendar year prior to the year or referral (affording a kind of "before" and "after" picture of VR services—a powerful indicator of the value of VR). These earnings data will be cross-classified by various characteristics found on the Form RSA–300 (age, sex, race, disability, etc.).

After RSA has received and carefully reviewed the tabulations, a memorandum will be forwarded to the State agencies spelling out the purpose of the data, how it was compiled, how it can be used, and other information on the data exchange that would be helpful to the States.

Regarding your concern for individual privacy of those clients receiving rehabilitation services, we can assure you that all information emanating from the data link will be so aggregated as to make it impossible to identify any individual. A "rule of five" will be enforced by SSA whereby earnings or other data will be shown only when available for at least five persons.) This will guarantee confidentiality and should in no way interfere with the willingness of certain programs to refer their clients for vocational rehabilitation services.

We hope this information will be helpful. If you have any further questions, please let us know.

Sincerely yours,

JOHN J. SZUFNAROWSKI,
Associate Regional Commissioner, RS.

DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE,
SOCIAL AND REHABILITATION SERVICE,
Washington, D.C., March 22, 1974.

To: State Rehabilitation Agencies (general), State Rehabilitation Agencies (blind), Associate Regional Commissioners, RS.

Subject: Deletion of names and addresses from the individual case service report, form SRS–RSA–300.

Content: Effective immediately, all State rehabilitation agencies sending client data on Form SRS–RSA–300 to the National Center for Social Statistics (NCSS) are required to delete the name and address of the client before they submit such forms. This is to insure the maximum degree of confidentiality of information on participants in the State-Federal rehabilitation program.

In this connection, I urge that all agencies still transmitting forms to the NCSS seriously consider sending only punch cards or tapes instead. This would be an added insurance against possible loss of client privacy emanating from the Federal level.

———— ————,
Acting Commissioner, Rehabilitation Services Administration.

CHAPTER VI

SECTION E

Form RSA–300 Case Service Report

I. PURPOSE AND SCOPE OF THIS SECTION

Statistical reporting under the Federal-State program of vocational rehabilitation is sponsored by the Rehabilitation Services Administration (RSA) and conducted under the auspices of the National Center for Social Statistics (NCSS). The statistical reports made by the State agencies enable both the Federal Government and the State agencies to measure the progress of the program and to evaluate its effectiveness.

The reports are designed to summarize the statistical data necessary to describe the various aspects of the program, to provide an adequate basis for sound planning, and to provide a minimum amount of uniform case progress information.

II. LEGAL BACKGROUND AND AUTHORITY

Section 5. (*a*) (*8*) of the Vocational Rehabilitation Act as amended through 1968, and Section 401.20 of the Regulations issued by the Secretary, January 18, 1969, relate to the submittal of reports. The National Center for Social Statistics functions as the collecting and processing agency for Rehabilitation Services Administration sponsored reports.

III. Case Service Report

A. *Purpose of the Case Service Report*

The Form RSA–300, "Case Service Report", revised July 1, 1969, replaces the Form R–300, "Case Service Report", revised July 1, 1966. It is designed to accumulate basic information about each individual in the rehabilitation process, and will be used: (1) as a tool for measuring the effectiveness of the rehabilitation program at National and State levels; (2) in describing the operations of the program to the Congress and to State Legislatures; (3) in estimating the cost and evaluating the effectiveness of proposed legislation; (4) for the dissemination of data on the characteristics of clients in the vocational rehabilitation program; (5) to provide data on the operations and effectiveness of the program to various public and private organizations interested in the vocational rehabilitation of the handicapped; and (6) to provide specific answers to questions which are frequently raised on operations of the program.

This is a comprehensive, standardized system of statistical reporting on the complete rehabilitation process for every individual coming into contact with that process, from first referral to final closure. The Form RSA–300 provides for reporting on the individual when first referred, when the referral process is completed, and when the case is closed from extended evaluation or from the active caseload. It is recognized that in some agencies the counselor will not have access to the cost of case services at the time he completes Part 3 of the form and that this information will be completed in the central office of the agency. However, once the cost of case services information has been added by the central office to the form, it can serve as a very convenient mechanism for those agencies wishing to keep counselors informed as to the costs of rehabilitation incurred for each of their clients. This can be done simply by returning the appropriate page of the form to the counselor with the financial data completed.

B. *Quality of Recorded Data*

It would be difficult to conduct a program for expanding and improving vocational rehabilitation services or to measure the effectiveness of expanded opportunities provided in new legislation without the data contained in the Form RSA–300. Evaluation of the data, however, can only be as valid as the recording and reporting of the data are accurate and reliable. It is essential, therefore, that each State agency insure that the utmost care be taken in maintaining accurate and complete data in case records and in the reporting on the Form RSA–300. While it is not required, it is suggested that State agencies make periodic sample checks of case files to assure itself of the quality of the data as reported on the Form RSA–300.

C. *Design of the Case Service Report*

The Form RSA–300 is designed to lend itself to a punched card or computerized system as well as to a manual system. It has been made as nearly self-coding as possible, with the intent of reducing to a minimum the necessity for the counselor or his secretary to have to *write* information. Almost all of the data can be completed either by a checkbox (pre-coded) or by a code entry, and nearly all of the codes are on the form itself.

The report is a three-part, five-page precarbonized form, designed so as to permit "flow" reporting while retaining in duplicate on the next succeeding page the information previously reported. The third, fourth, and fifth pages are duplicates and are a complete record of the individual's rehabilitation progress. Page 3 is the NCSS Statistical Copy, page 4 is the State agency copy, and page 5 is on heavier paper and is to be filed in the closed case folder.

The item identification design of the Form RSA–300 is sequential alphabetical designations beginning with the letter "A" within each of the three numerically designated parts. Item references will be by the "Part" number, followed by the alphabetical designations; i.e., Part 1, Item C, will be referred to as "1.C. Referral Date".

Except for disability and occupational coding, all necessary codes are printed on the back of the last page (page 5) of the form. For the disability codes, references must be made to Chapter 13 of the VR Manual. However, in printing Chapter 13, the portion concerned with disability coding has been designed so that those pages can be extracted from the VR Manual for desk use and for agency reproduction so that counselors and secretaries may each have a copy.

Occupational coding must be done by reference to Volume I, Third Edition, *Dictionary of Occupational Titles*. Large volume agencies may find it advantageous to extract the *DOT* occupation titles, descriptions, and four-digit code numbers of the most common job placements in third State onto one or two

sheets of paper and reproduce them for desk use by counselors and secretaries. This would reduce the necessity for constant reference to the *DOT*.

D. *Submittal of the Case Service Report*

The NCSS statistical copy (page 3) is to be held in the State office for periodic submittal to the NCSS.

E. *Use of the Case Service Report*

All agencies must use the Form RSA-300 in the *exact format* prescribed by NCSS (facsimile on page 13-2-53, A-F), unless they elect to submit the standardized punched cards (facsimile on page 13-2-53G), or standardized magnetic tapes (specifications available from NCSS on request). No substitutions or alterations of either the forms, punched cards, or tapes will be acceptable.

F. *Reproduction of the Case Service Report*

An initial supply of the new forms will be provided. Thereafter, agencies are required to arrange for printing of the forms themselves. The form must be printed as an exact replica; in at least the same number of copies, precarbonized, and snap-out. No items may be added or deleted nor may any other alterations be made.

G. *The Caseload Statuses*

There are 16 status classifications under the caseload status coding structure coded in even numbers beginning with 00 and ending with 30. The odd numbers, 01, 03, etc., have been excluded from the Federal coding structure to permit their use by those agencies desiring to record additional detail in case progress recording.

REFERRAL AND APPLICANT CASES

A referral is defined as any individual who has applied to or been referred to the VR agency by letter, by telephone, by direct contact, or by any other means; and for whom the following minimum information has been furnished: (1) name and address, (2) disability, (3) age and sex, (4) date of referral, and (5) source of referral.

It should be noted that *it is not intended to include in the definition of "referrals"* those individuals included in long lists of persons who are "screened out" by criteria established in a cooperative agreement between the VR agency and another agency such * * *.

STATE HOUSE, BOSTON—Governor Francis W. Sargent today directed the Massachusetts Rehabilitation Commission not to comply with Federal identification requirements. Under federal regulations states must submit to the Department of Health, Education, and Welfare the names, addresses or social security numbers of all applicants and/or recipients of vocational rehabilitation.

In a letter to HEW Secretary Caspar Weinberger, the Governor stressed the need to protect the confidentiality of clients' records and the privacy of persons in need of rehabilitative services. He notified Weinberger he is therefore directing the Massachusetts Rehabilitation Commission to substitute its existing numeral identification system for client social security numbers which are required by HEW.

The Governor also requested that appropriate federal action be taken to safeguard the confidentiality of records already collected on Massachusetts citizens. The Governor wrote:

"I share the concern (of the Massachusetts Rehabilitation and other public and private agencies serving the disabled) that the use of the social security number for identification threatens the confidentiality of individual client records and potentially compromises the value of rehabilitation services. Already a number of social service agencies in the Commonwealth have refused to refer clients for vocational rehabilitation because of this requirement. They are fearful that individuals, particularly those suffering from disabilities that have a social stigma attached, such as "drug addiction," or "Alcoholism," will suffer a residual impairment to functioning if their previous condition is widely recorded and possibly accessible. The collection of such information in a centralized, national data bank linked to the Social Security Administration can be viewed only with alarm."

As of June 1, 1974, Massachusetts Rehabilitation Commission had a case load of approximately 20,000 individuals, all of whom are covered by the federal reporting requirement. At the Governor's direction, Russell E. O'Connell, Commissioner of the Massachusetts Rehabilitation Commission has instructed Area and Regional offices of the Commission not to supply the names, addresses, or

social security numbers of rehabilitation recipients and applicants for inclusion in the HEW national data bank on the disabled.

HEW collects the social security number of MRC clients in order to link rehabilitation records with those of the Social Security Administration. This enables the federal government to monitor personal incomes of current and former clients receiving rehabilitation.

Although Massachusetts is the only state to date to take this action to protect the personal privacy and rights of the disabled, the Governor expressed confidence that other concerned states would follow suit and no federal rehabilitation funds would be jeopardized. The Commonwealth receives about $20 million in federal rehabilitation funds.

The Governor concluded: "I believe that we can meet the needs of your department to collect pertinent statistical data necessary for planning and program monitoring without sacrificing personal privacy and the confidentiality of client records."

JOINT TASK GROUP,
CONFIDENTIALITY OF COMPUTERIZED MEDICAL RECORDS,
July 1, 1974.

Mr. MARK BRAVIN,
Government Operations Committee,
U.S. Senate, Washington, D.C.

DEAR MARK: Enclosed are (1) the requested answers to the questions;
(2) two typical cases with obvious traumatic consequences;
(3) a prepublication copy of the presentations of Dr. Walters and Mrs. Kaiser at the recent 6th Buffalo Conference. If I can be of further help, please let me know.

I want to thank you for your splendid help in this matter during my visit as a witness.

Sincerely yours,

E. R. GABRIELI, M.D.,
Chairman, Joint Task Group on Confidentiality of Computerized Medical Records.

Enclosures.

Mary became worried because she felt tired, weak, she lost her appetite and her ambition to work. Mary went to the neighborhood health center. The examining physician inquired about her menstrual history. Mary stated that her last period was 6–7 weeks ago. The clinical diagnostic study justifiable included a full metabolic work-up and also a pregnancy test.

Mary's next door neighbor worked in the laboratory as a typist. She noticed that Mary's urine was tested for pregnancy. Soon, the word got around throughout the neighborhood that Mary is suspected of being pregnant. Several parents in the neighborhood no longer allowed their children, boys and girls, to associate with Mary. Finally the conservative rural community shared the "news" with the parents. Mary had to leave the community, her reputation was ruined. Mary knew that her chances of getting married, like all other girls, were lost. She committed suicide. The autopsy findings supported the neighborhood clinic's medical impression: hyperthyroidism, secondary amenorrhea.

The autopsy also confirmed Mary's claim: that she has never had any sexual intercourse. She was a virgin.

Dr. R. B. is a professor of obstetrics at a prestigious Southern Medical School. Virginia, a 17 year old high school girl, accompanied by her father, requested examination for her vague abdominal pain. The examination revealed that Virginia had an acute gonorrhea. Virginia was instructed, received penicillin injection, and confidentiality was promised pending on her cooperation. The Blue Shield sent a copy of the reimbursement form to the father, including the specification of the services rendered. The father noticed that an injection was given. He rushed to the gynecologist and demanded full explanation. The ensuing conflict between father and daughter, and the loss of confidence in privacy of medical information were both dramatic.

Question. In light of the public's right to know and need to know the health condition of public officials and candidates for public office, where would you draw the line between that right and the right of the public official to have his medical records kept confidential?

Answer. Public officials and political candidates should have the right to keep those medical records confidential which were prepared prior to their decision to

seek a public office. It should be a part of the preelection procedure to undergo a physical examination, given by an experienced physician recommended by the corresponding medical society (i.e., County, State, or National). Those parts of the preelection medical examination which may limit the physical/mental/spiritual performance of the candidate, should either be made public, or the candidate should withdraw from candidacy. This way he could still keep the findings private. Also, public officials should be examined regularly by a physician, chosen as above, and the potentially performance-limiting facts should be made public information.

Question. Are doctors under excessive pressure or harassment by Federal (and other) investigative agents to reveal information about patients? If so, should some steps be taken to strengthen the doctor's right to withhold information from investigators?

Answer. Generally, individual practicing physicians are not harassed by Federal agents to reveal information about patients, but there are numerous alarming exceptions. For instance, a psychiatric registry program sponsored by the National Institutes of Mental Health forces all institution-based psychiatrists to submit fully identified examination records. The State Health Department in Iowa, and recently in Missouri began to centralize all hospital discharge summaries, without instituting adequate data security measures. To some, it may seem more expedient to develop health data systems within governmental structures rather than to strengthen the doctor's right to withhold information and to establish independent, autonomous health data centers, in order to assure confidentiality of all clinical information. On the other hand, a free democratic society should be deliberately less efficient in the area of medical privacy, just as our judicial system is deliberately less efficient, in order to protect the innocent.

It may seem expedient to compare gun license applications with a computer-produced lists of all psychiatric patients, but in reality the yield is low, and the risk is high: as soon as patients will learn that their psychiatric consultations are no longer confidential, the patients will no longer trust their doctors, loss of confidence will destroy psychiatry. Those states which began recently to use medical information for criminal investigations should no longer be allowed to continue with such methods. Medicine should be separated from criminal evidence gathering.

Privacy and Medical Record-Keeping

(By Barbara L. Kaiser)

In the middle of May, of this year, Tom Wicker ran two columns in the New York Times that succinctly and vividly depict what can happen when a comprehensive data storage and retrieval system for personal data goes into operation without an adequate set of safeguards prepared in advance.

The system in question has been in operation in Sweden for a number of years. It actually exists as an instrumentality of social welfare in a socialist society, and it contains, and gives out, all kinds of data, including medical records. Each Swede has an identification number assigned at birth, and this number serves as the code key that indexes all the stored data. Sweden also has, according to Wicker, a tradition of open and available public documents; the tapes and other equipment upon which the stored information is recorded are regarded as public documents. The consequence of this is easy enough to perceive. Until quite recently, anyone at all, with or without what lawyers in this country might call "standing," could go to the appropriate government office and obtain any set of records on anyone, for any purpose at all. Moreover, in 1970, the national census data were computerized, and all the tapes went on unrestricted sale.

Americans concerned with concepts of privacy that are just now struggling to become established as constitutional tradition may shudder at the thought of what destruction the Swedish system would wreak on, for example, the law emerging from the *Griswold* case and the 1974 Supreme Court decisions on abortion. In fact, if Wicker's account is correct, the Swedish system of record keeping was in effect for quite some time, without much to-do over invasion of personal privacy, until the tapes of the census data were put on sale, simultaneously with moves in the Parliament to set up a central register of all available personal data on every citizen. This comprehensive system never came into existence, for political reasons as it appears, but the public outcry the proposal engendered

caused the government to establish, instead, a commission to examine the effects of central computerized data storage and retrieval systems on personal privacy. In consequence of the work of this commission, there has been enacted a law regulating the use of personal data in the public system, with limitations on the availability of the data spelled out, and a government agency established to supervise administration.

As should be apparent, it may well be that the Swedes have locked the stable door after the horse has been stolen. The free availability of data up to the present time has made it possible for private enterprise—which does exist, even in the welfare state—to make and use mailing lists in exactly the same way as the same thing is done in this country. With the lists in private possession, it becomes extraordinarily difficult to control their use, and to give unsuspecting private individuals any protection against having their names exploited commercially or against having all manner of private information concerning themselves published in places where they would not choose—if they had the choice—to have that information go. One of the examples of such exploitation that Wicker uses is that of the new mother in the hospital, two days after delivery, flooded with mail addressed to her by name and having the sex of the baby correct, advertising everything possible for the baby, sent out by business concerns that have had access to the central lists.

From all of this it is abundantly clear that unless the perils of computer technology are anticipated along with its benefits, we can all be living in glass houses with glass interior walls, and the concepts of privacy and confidentiality can become quaint relics of the horse-and-buggy era. The Swedish experience, and the measures taken to bring the situation under control, can profitably be used to demonstrate that it is always later than we think and that in fact we are not likely to overstate the dangers. That is why meetings such as these are a genuinely welcome event. They show a wise concern with preventing the technological capability of computer data storage and retrieval systems from so far outstripping the effective protection provided for personal privacy that the situation gets completely out of hand and no real remedy is possible.

It is worth while at this point to consider what factors are involved in the establishment of record systems that reconcile the patients' rights to privacy with the benefits of computer technology. There is probably no need to expand much on what these benefits are. A few that come to mind are: ready availability of the records, speed of retrieval, ease of assimilation of the data into widely varied statistical systems, protection against loss, the possibility of sharing information among providers of health care, the possibility of getting up comprehensive medical biographies of patients so as to improve care, the possibility of adaptation of rcorded information for diagnostic purposes, with consequent expansion of medical knowledge.

It is, however, the human cost of realizing all these benefits with which we must concern ourselves, a cost that may express itself in terms of the loss of certain rights that our Constitutional system establishes as extremely valuable. The rights we are dealing with are those we may lump together under the general heading of privacy, although there is one threshold issue that must be dealt with before the actual question of privacy can be tackled.

That threshold issue arises out of the relation between the doctor and the patient as it has come to exist in this year of grace, and is the question of the extent of the patient's right to see and have copies of his, or her, own records. It is an extraordinary fact that among all the kinds of personal records kept on people in all the many social and economic relationships where records are required to be kept, there are two kinds that are routinely made unavailable to the persons about whom the records are made. One is the set of records made about students in schools, particularly primary and secondary schools, and the other is medical records. The reasons customarily advanced for excluding people from access to their own records are strikingly similar in both cases: that is, it is said to be for the subject's own good.

It would be inappropriate in this context to go into the question of school records, but the question of patients' access to their own medical records is of the first importance in connection with any effort to set up a proper ethical medical data center. As a rule, medical records are made as an adjunct to the delivery of health care, but there may be many other reasons for the making of a medical record. These include determining eligibility for insurance; deciding whether someone meets job qualifications, should be granted or is ready to return from sick leave; fulfilling the conditions for engaging in competitive

interscholastic sports; settling upon whether a discharge from the armed services should be granted and, if so, on what grounds; sentencing convicted criminals; adjudicating questions of child custody; making family court dispositions on petitions of child neglect or abuse, family offenses or for adoption. The list can go on much longer, but enough items have been included to suggest how many and varied are the situations that may give rise to a medical record.

Medical records have two characteristics that set them off from many other kinds of records, although the differences may not be so great as they superficially appear to be. First of all, medical records are as a rule not made by the patients themselves, nor are they made for the patient's use. They are made by doctors, nurses, technicians, therapists and other medical, para-medical and auxiliary personnel.

In any case, whatever the purpose for which the records are made, with very few exceptions the patients do not generally ever have physical possession of the records concerning themselves. If they are to see the records at all, they must ask someone for them.

The second important characteristic of medical records is that they necessarily include highly intimate data about the patients, of a kind that the patients might never reveal to anyone except, so to speak, "under the seal of the confessional." This data is often given (and the word "given" is, of course, intended to include what is found on examination as well as what is expressed by word of mouth) when the patient is ill, and needs to establish a dependency relationtionship with a medical attendant. But the data may also be given in the course of routine physical examinations for any of the kinds of purposes mentioned heretofore, when the patient is not ill at all, or it may emerge in the course of prenatal care of obstetrical patients, most of whom are, and remain, in quite good health.

The usual response, when patients ask to see their charts, is negative. Particularly stubborn patients can sometimes succeed in gaining access, but as a rule permission is refused and the patients acquiesce. There are a few exceptions to this rule. In Massachusetts an express statutory right of access to their own records is given to all patients except those in mental hospitals. And a few hospitals with academic connections have sponsored experiments in bringing patients into the record-making process as participants and sending them home with complete copies. Papers describing this adventurous approach to medical record-keeping have come out of Yale and the University of Vermont. Both sets of writers regard the experiment as a success, not only in terms of establishing good doctor-patient relations, but also as a positive contribution to the quality of health care.

Normally, however, the record is regarded as owned by whoever is the custodian. This position may be expressly set out in writing, as it is in the manual of instuctions of the Kaiser-Permanente Hospitals in California, or it may simply be the assumption underlying the behavior of the staff and the records librarian. Ownership being, by definition, the power to prevent others from having or using the object owned, it is regarded as sufficient legal justification for excluding patients from access to their records. The matter of ownership becomes more complex if the records are maintained in more or less autonomous data banks, especially when the bank is a central facility fed from and used by a number of institutions. Possibly, under the ownership theory, the storage facility would be regarded as a trustee for the hospitals, which would still consider themselves owners, to the exclusion of the patients.

Other reasons are given to rationalize and justify keeping patients from access to their records. One that is frequently used is that the records are made in technical language that the patients would not understand. This argument sometimes goes on to make the further point that patients, not understanding what the record says, will misinterpret what they read, and indulge in dangerous activities such as self-medication. Accordingly, patients should be told only what their doctors think they ought to be told: the doctor is the best judge of what information a patient ought to receive.

The answer to this argument is that what patients do not understand can be explained to them, and that doctors who take seriously the need to obtain genuinely informed consent to procedures and treatment ought to be prepared to make the necessary explanations.

Patients who are reasonable people will not then be disinclined to follow the instructions of their physicians because they have seen their charts; on the contrary, they will know better what they are to do because they will know why. Patients who are not reasonable people will not be made to behave reasonably by

being refused access to their records. And the status of being a patient does not automatically justify being treated like an incompetent. One may know nothing of higher mathematics or Hungarian but a librarian would not be justified in refusing to loan a book on calculus or Magyar language to a borrower because of this ignorance. The borrower might want the book for the purpose of learning what he does not know. Similarly with the charts of a patient.

The other chief reason for withholding access of patients to their own records is that there may be material in the records that it would harm the patient to see. The unusal examples given are fatal prognoses written into the charts, or diagnoses of malignant disease. Some psychiatrists make the related argument that in the course of treatment they need to interview third persons, who would not speak freely if they thought the patients themselves would find out what they had said.

Whatever validity there may be in this position in some instances, it is an argument that goes too far and proves too much. If for example a woman in good health visits the doctor for a series of prenatal visits, and then has a normal delivery of a healthy baby, it seems hardly likely that her records would contain any information it would harm her to receive. The same is true of someone who comes in with a broken bone, a ruptured appendix, a pair of infected tonsils, or any of a myriad of possible conditions that might bring a patient to a doctor. It is also true of a patient who comes in already knowing that he or she has a malignant disease or a fatal prognosis. Although in some instances showing patients their records might demonstrably be harmful to them, it is surely not sufficient to justify a blanket prohibition on patient access to records. The related point is sometimes made that most people would rather not try personal right of the physician to the privacy of his or her own speculations to understand the technicalities of what is wrong with them.

The arguments for routinely allowing patients access to their own records on request rest, it seems, on a firmer foundation than the arguments to the contrary. From the legal point of view, there is no justification for treating a legally competent person as if he or she were incompetent. The doctor-patient relationship, though it often entails a dependency of the patient on the doctor, does not constitute the doctor the patient's committee. From the point of view of the civil libertarian, there is no overriding state interest that would justify the exercise of censorship over what a patient may read. Moreover, there is a substantial distinction between the records as pieces of physical property—as to which ownership in the custodian can be conceded—and the records in their aspect as information. In this latter aspect it may be of crucial importance to the patient to have it, and may do him or her a grave disservice to have it withheld. Patients should know, for example, what drugs they are being given or have had: to protect themselves against allergic reactions, for example, or * * * about side- and after-effects. The recent stir about the carcinogenic effects of diethyl * * * gestrol on daughters * * * been given the drug in pregnancy is * * * example * * *.

Most of the arguments in favor of giving patients access to their own records seem to be based on the tacit assumption that the interests of the patients and that of the donors, the hospitals or any other cusodians of medical records are sufficiently identical so that the custodians can be trusted with the job of protecting the privacy rights of the patients in their records even when the patients are kept from knowing what the records contain. This is a complete assumption, false in many respects. It runs contrary to the tenor of most of our law, which normally * * * the owner * * * right the proper party to assert it and protect it, and only exceptionally gives that power to a surrogate.

Health care personnel—doctors, nurses, para-professionals and others—and hospitals in New York are bound by an evidentiary privilege not to reveal confidential information in the medical records of a patient unless authorized by the patient or unless the patient has waived the privilege. The privilege is statutory, and is a feature of the doctor-patient relationship. It can be enforced by court ruling in a lawsuit, but the existence of any other remedies in case of violation is rather doubtful. Even assuming, however, that the law created an unconditional obligation on medical personnel, and provided remedies, for enforcement, as it does in some states (Connecticut, Maryland and Massachusetts, to name some), there would remain some important problems arising from the non-access of patients to their own records.

One fairly obvious problem is that of making sure the records are correct. It is not unknown that two patients should have the same name and that their records should therefore be confused. It is not impossible that an incorrect entry

37-583 O - 74 - pt. 2 - 59

should be made in a chart, or that something should be omitted. The possibilities for error are endless, and so are the possibilities for harm resulting from such errors. Patients have the best reason of anyone to detect mistakes in their own records and press to have them corrected.

It does not so readily come to mind in considering medical records that they are often in the hands of someone who does not owe the patient any duty of confidentiality at all: an insurance company, or an employer, or a school, for instance, any of which may have required a physical examination, more or less thorough but in any case generating a medical record, as a condition for granting something that the examinee was applying for. Or the records, originally with a hospital having a duty to maintain confidentiality, may be released to a third party with a contractual obligation to finance care, pursuant to a waiver solicited by the hospital upon admission of the patient. It may be necessary that the patient's records be released in this way, but in so doing the patient effectively loses all privacy rights in the records. If then the records can be withheld from the patient by a subsequent custodian (who may very well claim this right derivatively from the treating physician), the grotesque result may be that the patient is the only person who cannot have access to his or her own records; there is nothing to stop this custodian from releasing them in response to any request, errors and all.

At least as serious as the question of possible error in the records, which patients ought to have opportunity to correct, is the fact that there may be a genuine adversity of interest between the patient and the custodian of the records. We have heard a good deal, in recent months, on the subject of the propriety of the President's deciding for the House of Representatives what evidence it should consider in proceedings leading to impeachment. The same incongruity may be present in leaving it to doctors and hospitals to decide what information a patient may have concerning himself, if the question is one of malpractice. In the homely words of the common expression, it is like setting the fox to guard the chicken house.

Finally, the question of patients' access to their own records has a very important bearing upon the question of the effective protection of the privacy of these records. That right of privacy belongs only to the patient, the subject of the records. It is not a right belonging to the doctor, or any memer of the health care staff, or the hospital, or any third party who may happen to have custody of the records, and, as has been pointed out, none of these persons, organizations or institutions is necessarily motivated to protect the right. On the contrary, each may have its own interest in invading the patient's privacy, and that interest is likely to be very well served by keeping the records out of the patient's hands. The patient alone is fully motivated to protect his or her own privacy rights but those rights are self-evidently illusory if the patient has no way of learning at first hand the concrete content of what is to be protected.

This last consideration is the one which is most closely connected to the questions involved in the establishment of an "ethical" computer data storage and retrieval system. The term "ethical" presumably describes a system in which maximum protection is accorded to the rights of patients to the effective safeguarding of the intimate information that is inevitably developed in the course of health care delivery. In essence, the privacy problems that must be solved for such a system are really much the same as those involved in the horse-and-buggy records library with file folders in ranks in file cabinets, except that they are on a much larger scale. Simply stated, they are: (1) How to keep the records out of the hands of unauthorized third parties. (2) How to make the records available for use by the providers of health care, to the maximum benefit of the patient: and (3) How to determine what third persons (other than the health care personnel) should be entitled to see and use the records, and under what conditions this should be permitted. Most of the questions that arise relating to the privacy interest in these records can be subsumed under one or another of these heads.

For the sake of confining the discussion within management limits, privacy will be generally considered to refer to the ability of a person who is the subject of medical records to prevent the information in those records from coming into the hands of persons not entitled to have it. The law of the State of New York does not by any means give unqualified recognition to this right.

In the event of litigation, a patient may have the benefit of a statutory rule of evidence that excludes information secured by doctors within the confidential doctor patient relationship. Like most rules that have been elaborated in case law, this one is hedged about with qualifications and provisos, some of which tend

seriously to erode the scope of the patient's right of privacy, but this is a matter that need not be gone into here.

Outside the context of litigation, however, there is not much effective or reliable protection for the patient's right of privacy. The nearest the law seems to come to offering a direct remedy for violation of a duty to maintain medical records confidential is a tort action for invasion of privacy. In the absence of a clear statutory duty, such an action is a gamble by the patient. Among the obvious hazards is, for example, the possibility that he or she might not even learn of the violation of the privacy right until the statute of limitations had already run out, by which time, of course, the information would be irrevocably in the hands of an incalculable number of unauthorized persons.

In the second place, hospitals commonly require patients, upon entrance, to sign a paper that may be variously denominated a release, or a consent form, or an authorization. One provision often contained in a paper of this sort is a blanket permission to the hopsital to release records of the patient to any third party under contract to finance the patient's medical care. The patient who signs such a provision as this has effectively given up privacy rights, because, although the hospital and its staff and the health care personnel may be scrupulously careful in respecting the confidentiality of the patient's records, once these records have been turned over to the person contracting to finance the care, there is no further restraint on the dissemination of the information. Confidentiality is a by-product of the doctor-patient relationship. It does not inhere in the relationship betwen the patient and the insurer of hospital bills. The insurers have their own pooled data system—the Medical Information Bureau—and patients have no way of knowing what information may have found its way into this system, nor any way of controlling the uses of that information.

But leaving aside the questions of the waivers of privacy secured from patients, and the collateral consequences of these waivers, it is possible to consider in relatively simple terms what kinds of protection are necessary for the privacy of the patient, consistent with the other legitimate purposes to which the records can be put, such as facilitating the delivery of health care, the furtherance of scientific knowledge and serving certain carefully defined needs of government. When the nature of these protections has been delineated, it should be possible to determine how to regulate a computer data system so that it will conform to genuine ethical norms.

Meaningful protection to the patient's privacy rights really requires that access to the records in the hands of any custodian at all should only be given to carefully defined classes of recipients. In order for this protection to be genuinely effective, the concept of a custodian of medical records would have to include any person or organization, whether publicly or privately maintained, that stores records of this kind for any purpose. It would include not only custodians within the control of doctors, hospitals and other providers of health care but also employers, schools, insurance companies and any other persons, organizations or institutions that maintain files of medical records, whether or not there exists any confidential relationship between whoever maintains the files and the persons who are the subjects of the records. It would certainly include independent facilities for medical record storage and retrieval, such as are contemplated in this conference.

It is not really a simple matter to define those who would be entitled to access to the records, and the suggestions offered here do not pretend to either exhaustiveness or finality. Obviously, in light of what has already been argued, the subjects of the records themselves must be permitted access on request, and those persons who are specifically authorized by the subjects. How to safeguard records against misuse of such authorization is a practical problem that can be met with such commonsense measures as requiring written permission, with specification of the records to be seen, and adequate identification of any applicant for access.

More difficult problems arise in cases where there is a genuine need for access to the records, and it is impracticable to obtain the subject's prior consent. One such instance is the use of medical records for scholarly investigation. No privacy right seems to be invaded if the published results are in statistical form, or do not in any way identify the patients. On the other hand, if the patient is inevitably to be personally identified in the investigative report, it seems reasonable to require that his or her permission should be requested prior to publication, and that without it the material ought not to be used.

Law enforcement needs always give rise to some difficulties, but it is possible at least to recognize distinctions between those which must be made paramount and those which can and should be subordinated to the patient's privacy rights. For example, effective control of communicable disease may absolutely require that health department officers, or their equivalents, have access to patients' medical records and be able to identify the patients. On the other hand, the requirement that doctors who treat gunshot wounds report each such instance to the police, while customary, is of doubtful defensibility. The involuntary sacrifice of the patient's privacy, and possibly also of his constitutional rights against self-incrimination, is probably not outweighed by the benefits to law enforcement in such cases.

Some recent New York cases nicely illustrate the problems of reconciling legitimate law-enforcement needs—in this instance the collection of vital statistics by health departments—with patients' privacy rights. The patients in these cases were women who had had abortions. Health Department regulations required the attending physicians to file fetal death certificates giving, among other data, the names and addresses of the mothers. These rquirements were attacked as invasions of the women's rights to privacy. In one case, a Supreme Court in New York City sustained the challenge. In the other, in another part of the state, the Supreme Court held that the privacy right was outweighed by the State's interest in collecting the information, but it refused to enforce the rule against a doctor who had violated it because the Health Department was too lax in protecting the privacy of the information thus obtained. The first of these cases has now been decided on appeal in the Appellate Division for the First Department. The latest pronouncement is that the invasion of the patient's privacy by a rule of this sort is justified.

One more serious problem of the privacy of medical records is how to handle efforts to subpoena medical records for use as evidence. As to this, probably the best solution—no matter who may be the custodian of the records in the particular instance—is to require that the party seeking to secure the records by subpoena give the patient notice of the issuance of the subpoena, and to permit the patient to contest its enforcement by whatever means is regarded as satisfying the requirements of due process. Cases of this kind can then be decided on the basis of the nature of the particular claim for the record, in the traditional adversary manner.

The practical problems of protecting the privacy of recorded medical information are legion. They proliferate with the development and the increased sophistication of data storage and retrieval systems, and record-keeping develops a life of its own that is less and less easy to control. An approach through general legislation, directly tackling the privacy question and defining rights and remedies—somewhat after the manner of the Federal Administrative Procedure Act, or the Freedom of Information Act—seems to be the most promising route to the provision of effective protections. Some of the recent Federal enactments setting up categorical substantive programs that generate or use medical records, such as the laws establishing programs for controlling drug abuse, do contain some privacy protections, if only in recognition that the target populations that the laws seek to reach would be discouraged from using the facilities if the confidentiality of the records were not faithfully maintained. Indeed, it might be a good idea, in any case, to survey any such new legislation for its impact on privacy rights. But legislation generally applicable to all medical record-keeping, with well-thought-out terminology and definitions, could provide a useful broad framework of privacy rights into which then most categorical and special legislation could be fitted.

An interesting legislative proposal from this law school, specifically aimed at computer storage and retrieval systems, seems to treat these facilities pretty much as if they were public utilities, and would place them under regulation by government agencies. There are other proposals that would simply establish a system of substantive privacy rights and remedies for all persons who are the subjects of medical records. These two types of legislative schemes can be made to co-exist; and with the benefit of competent draftsmanship, they might be mutually reinforcing, providing for the first time a serious, self-conscious and workable definition of privacy rights in an extraordinarily important and sensitive area of people's lives. It may be that technology and entrepreneurial genius will always be a little ahead of the personal rights they threaten, but efforts such as this conference can at least keep the distance reasonably short by focusing sharply on the subject that is most likely to be forgotten in our industrial society: that is, the very important individual human being.

MAILING LISTS

JUDICIAL DECISION

Lamont v. *Commissioner of Motor Vehicles*

Corliss Lamont, on behalf of himself and all other similarly situated, Plaintiff, v. Commissioner of Motor Vehicles and R. L. Polk & Co., Defendant. No. 67 Civ. 1540.

United States District Court, S.D. New York, June 22, 1967.

Action for declaratory and injunctive relief, and for money damages, based upon asserted unconstiutionality of statute. Plaintiff moved for the convening of a three-judge court and defendant opposed urging that complaint be dismissed by single judge. The District Court, Frankel, J., held that claims of privacy violations and deprivations of liberty and property under Constitution concerning statute authorizing sale of copies of motor vehicle registration records by the Commissioner of Motor Vehicles, which allegedly led to considerable annoyance and inconvenience from merchandise solicitation through the mails, by telephone and in person, were plainly unsubstantial, precluding convening of a three-judge district court.

Motion to convene three-judge court denied, and complaint dismissed.

1. Declaratory Judgement ⇐124
Injunction ⇐85(2)
Torts ⇐8

Right of privacy violations or deprivation of liberty or property under Constitution could not be invoked as basis for declaratory or injunctive relief, or for money judgment, upon asserted unconstitutionality of statute authorizing sale of copies of motor vehicle registration records by Commissioner of Motor Vehicles which allegedly led to considerable annoyance and inconvenience from merchandise solicitation through the mails, by telephone and in person. Vehicle and Traffic Law N.Y. § 202, subd. 3; U.S.C.A. Const. Amends. 1, 4, 5, 9, 14.

2. Courts ⇐101

Fact that a claim is novel does not in itself brand it as unsubstantial on motion to convene a three-judge district court. 28 U.S.C.A. §§ 2281, 2284.

3. Courts ⇐101

On a motion for the convening of a three-judge district court, the nonmethematical task of the single judge is to decide only whether the contention has some plausible chances of success, arguably sufficient to warrant full-scale consideration in the Supreme Court on an appeal as of right from a three-judge district court. 28 U.S.C. §§ 2281, 2284.

4. Courts ⇐101

Claims of right of privacy violations and deprivations of liberty and property under Constitution concerning statute authorizing sale of copies of motor vehicle registration records by the Commissioner of Motor Vehicles, which allegedly led to considerable annoyance and inconvenience from merchandise solicitation through the mails, by telephone and in person, were plainly unsubstantial, precluding convening of a three-judge district court. 28 U.S.C. §§ 2281, 2284; Vehicle and Traffic Law N.Y. §§ 202, subd. 3, 401; subd. 2; U.S.C.A. Const. Amends. 1, 4, 5, 9, 14.

Rabinowitz & Boudin, New York City, for plaintiff; Leonard B. Boudin, Joan Goldberg, New York City, of counsel.

Louis J. Lefkowitz, Atty. Gen. of State of New York, New York City, for defendant, Commissioner of Motor Vehicles; Mortimer Sattler, Asst. Atty. Gen., of counsel.

Royall, Koegel, Rogers & Wells, New York City, for defendant, R. L. Polk & Co.; Wyllys S. Newcomb, John M. O'Hara, Russell H. Beatie, Jr., New York City, of counsel.

OPINION

Frankel, District Judge.

Suing for himself "and all other owners of motor vehicles duly registered" in New York, plaintiff seeks declaratory and injunctive relief based upon the asserted unconstitutionality of N.Y. Vehicle and Traffic Law, McKinney's Consol. Laws, c. 71, § 202(3), which provides that the Commissioner of Motor Vehicles,

> "may, in his discretion, contract with the highest responsible bidder to furnish copies of records of all vehicle registrations for any registration period, or number of periods not exceeding five years in the aggregate, with respect to a given territory. In such event, the fees provided by this section [for searching and supplying copies of such records] shall not apply to copies of records furnished under any such contract."

The defendants are the Commissioner of Motor Vehicles and R. L. Polk & Co., which is said to be in the business, *inter alia*, of compiling directories and is alleged to have acquired the registration records as "the highest responsible bidder" under the statute. In addition to seeking a declaration that § 202(3) is unconstitutional under the First, Fourth, Fifth, Ninth, and Fourteenth Amendments, along with an injunction "restraining the enforcement and operation" of the statute, plaintiff asks for a judgment of $10,000 against defendant Polk. The court's jurisdiction is said to rest upon 28 U.S.C. §§ 1331, 1343(3), 2201, 2202, 2281, and 2284; 42 U.S.C. § 1983; and the foregoing Amendments to the Federal Constitution.

Plaintiff has moved for the convening of a three-judge court under 28 U.S.C. §§ 2281 and 2284.[1] Defendants oppose the motion, urging that the asserted constitutional issue is "plainly unsubstantial," Ex parte Poresky, 290 U.S. 30, 32, 54 S.Ct. 3, 78 L.Ed. 152 (1933); cf. Bailey v. Patterson, 369 U.S. 31, 82 S.Ct. 549, 7 L.Ed.2d 512 (1962), and that the complaint should, accordingly, be dismissed by a single judge.

The allegations generating these opposing views—taken as true, of course, for present purposes—are: that plaintiff and others like him are compelled to register their motor vehicles with the Commissioner; that defendant Polk, having acquired the registration records, uses the names itself, or sells or leases the lists to others, "for the solicitation through the mails, by telephone and in person, of the registered owners of vehicles, for the purchase of merchandise;" and that the result has been "considerable annoyance, inconvenience and damage to the plaintiff and other registrants by reason of the large volume of advertising and crank mail and other solicitation to which they are subjected." Defendants' actions and the provisions of § 202(3), the complaint concludes, "are in violation of the right of privacy of the plaintiff and other registrants, and constitutes [*sic*] deprivation of their liberty and property under the First, Fourth, Fifth, Ninth and Fourteenth Amendments to the United States Constitution."[2]

In support of the view that the constitutional issue he raises is sufficiently substantial to warrant the attention of a three-judge court, plaintiff's able counsel presents written argument which reads in its entirety as follows:

> "The substantiality of the constitutional question raised by the complaint in this case is shown by the recent cases dealing with the sanctity of a man's home and the privacies of life. Griswold v. Conn., 381 U.S. 479 [85 S.Ct. 1678, 14 L.Ed.2d 510]; Mapp v. Ohio, 367 U.S. 643 [81 S.Ct. 1684, 6 L.Ed.2d 1081]; Breard v. [City of] Alexandria, 341 U.S. 622 [71 S.Ct. 920, 95 L.Ed. 1233]; Public Utilities Comm'n v. Pollack [*sic*], 343 U.S. 451 [72 S.Ct. 813, 96 L.Ed. 1038]; Monroe v. Pape, 365 U.S. 167 [81 S.Ct. 473, 5 L.Ed.2d 492]; Frank v. [State of] Maryland, 359 U.S. 360 [79 S.Ct. 804, 3 L.Ed.2d 877]; Skinner v. [State of] Oklahoma], 316 U.S. 535 [62 S.Ct. 1110, 86 L.Ed. 1655]."[3]

To be sure, brevity, a somewhat rare delight in courthouses, is not to be discouraged by equating it with "unsubstantiality." It should also be observed that counsel argued engagingly, and at considerably greater length, in oral support

[1] Plaintiff's motion papers also request a preliminary injunction, but it was stated upon argument that this application is not being pressed at this time, pending the ruling on whether a three-judge court is appropriate.

[2] There is no allegation that plaintiff has demanded exclusion of his name from the list sold by the Commissioner. In response to the court's inquiry, the State Attorney General has taken the position that this is immaterial in any event. With that representation, the question is treated on the premise that such a demand by the plaintiff would have been futile.

[3] Plaintiff's Memorandum of Law, pp. 5–6.

of the view that expanding judicial concern for "the privacies of life" shows enough movement in the law to preclude dismissal of his complaint as frivolous. In the end, however, plaintiff's single sentence of written argument, followed by the citation of seven cases, among which one hurts him and six are inapposite, may fairly be taken as the legal measure of his novel claim.

It would be pedantic to linger over the many distinctions between this case and those involving searches and seizures (Mapp v. Ohio, supra; Monroe v. Pape, supra; cf. Frank v. State of Maryland, supra [4]), the sanctity of the marital relationship (Griswold v. Connecticut, supra), the power of States to *limit* solicitation (Breard v. City of Alexandria, supra), and laws for compulsory sterilization (Skinner v. State of Oklahoma, supra). The citation closest to the mark in plaintiff's list is Public Utilities Comm'n v. Pollak, and that is adverse to him. There, the dispute was over governmental approval of radio broadcasts, including commercial messages, to the captive audiences in publicly franchised buses and street cars. The intrusive assault upon the privacy and serenity of unwilling listeners forced to use public conveyances was so jangling to one normally hardy "victim" on the Supreme Court that he found himself unable to rule dispassionately upon the constitutional issue. 343 U.S. at 466–467, 72 S.Ct. at 822–823 (Frankfurter, J.). The Court majority pointedly recorded (p. 465, 72 S.Ct. p. 822) its expression of "no opinion as to the desirability of radio programs in public vehicles." The Court then proceeded, however, to reject the claim that the outraged listeners could invoke the right of privacy or other constitutionally protected interests to shut out the radio broadcasts. Mr. Justice Black dissented in part on grounds that give little or no comfort to the plaintiff in his case. The dissent of Mr. Justice Douglas, centering on the right of privacy, distinguished "the man on the streetcar," forced to hear the broadcasts, from the person at home who is free to turn off or away from an offensive program. Id. at 469, 72 S.Ct. 813.

[1] Strictly speaking, that decision is not squarely in point. It contains important implications, however, that lead *a fortiori* to the defeat of this plaintiff's claim. There is no captive quality in the plight of which plaintiff complains. The mail box, however noxious its advertising contents often seems to judges as well as other people, is hardly the kind of enclave that requires constitutional defense to protect "the privacies of life." The short, though regular, journey from mail box to trash can—for the contents of which the State chooses to pay the freight when it facilitates the distribution of trash—is an acceptable burden, at least so far as the Constitution is concerned. And the bells at the door and on the telephone, though their ring is a more imperious nuisance than the mailman's tidings, accomplish more peripheral assaults than the blare of an inescapable radio.

The information sold by the Commissioner is not vital or intimate. It is, moreover, in the category of "public records," available to anyone upon demand. See Vehicle and Traffic Law § 401(2). Indeed, questions more troublesome than plaintiff's might arise if the State adopted a policy of "privacy" or "secrecy" with respect to such information.[5] What the State has done in practical effect is to tap a small source of much-needed revenue by offering a convenient "packaging" service. This may not be the most inspired kind of government function, although it may be noted that eighteen other States appear to have adopted similar practices.[6] The point of importance, whatever aesthetic or other judgments might be prompted by this activity, is that it reflects a rational and allowable balancing of values by the elected representatives of the people.

In his contrary thesis, plaintiff proposes to stretch the constitutional dimensions of "privacy" far beyond any reasonably foreseeable limits the courts ought to enforce. His claim is in an area where there is no invidious discrimination, no problem of a wrong unreachable at the polls, no suggestion of an affliction confined to a relatively helpless minority. Cf. Reynolds v. Sims, 377 U.S. 533, 553, 84 S.Ct. 1362, 12 L.Ed.2d 506 (1964); West Virginia State Board of Education v. Barnette, 319 U.S. 624, 638, 63 S.Ct. 1178, 87 L.Ed. 1628 (1943). His alleged injury, shared with what is probably a majority of the electorate, results from a judgment by the State which appears to be well within its "vast leeway in

[4] Overruled in Camara v. Municipal Court, 387 U.S. 523, 87 S.Ct. 1727, 1741, 18 L.Ed.2d 930 (1967).

[5] Compare the Act of July 4, 1966, 80 Stat. 250, amending Section 3 of the Administrative Procedure Act to expand the availability of agency records and providing, *inter alia*, that "the burden shall be upon the agency to sustain its action" when it resists disclosure.

[6] Cal. Vehicle Code Ann. § 1811 (West Supp. 1966; Conn.Gen.Stat.Rev. § 14–19 (r) (1958); Fla.Stat. § 319.25(5) (a), F.S.A. (1965); Ill.Rev.Stat. ch. 95½, §

the management of its internal affairs." Sailors v. Board of Education, 387 U.S. 105, 109, 87 S.Ct. 1549, 1553, 18 L.Ed.2d 650 (1967).

[2–4] Of course, the fact that a claim is novel does not in itself brand it as unsubstantial. Cf. Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123, 159, 71 S.Ct. 624, 95 L.Ed. 817 (Frankfurter, J., concurring). The non-mathematical task of the single judge in a case like this is to decide only whether the contention has some plausible chance of success, arguably sufficient to warrant full-scale consideration in the Supreme Court on an appeal as of right from a three-judge district court. Perhaps "unsubstantiality" need not be so plain when a single judge dismisses as it should probably be when a single judge finds the *defense of constitutionality* frivolous (Bailey v. Patterson, supra) and then enjoins enforcement of the state statute. In the latter situation, the protection of three-judge deliberation is withheld though the case is squarely within the primary purpose of the scheme—"that a single judge ought not to be empowered to invalidate a state statute under a federal claim * * *." Id., 369 U.S. at 33, 82 S.Ct. at 551, 7 L.Ed.2d 512; and see Green v. Board of Elections, supra, 380 F.2d at 452. But where, as in this case, a single judge finds the plaintiff's contentions plainly unsubstantial, the normally less major consequence of error is at most to postpone invalidation of the State's law. And that, in the circumstances of this case, is a bearable possibility.

For the reasons above stated, the motion to convene a three-judge court is denied. The motions to dismiss the complaint are granted. The complaint is dismissed.

So ordered.

3–418 (1959); Ind.Ann.Stat. § 47–2625 (Burns' Replacement 1965); Mich. Comp. Laws Ann. § 257.232 (1967); Minn.Stat. Ann. § 168.33, Subd. 3 (1960); Mont.Rev. Codes Ann. § 53–101(8) (1947); Ohio Rev.Code Ann. § 4503.26 (Page 1965); Okla.Stat.Ann.tit. 47, § 22.24 (1962); Pa.Stat.Ann.tit. 75, § 417 (1960); S.C. Code Ann. § 46–120 (1962); Gen. & Special Laws of Texa , Chap. 720 § 36 of H.B. 12 (59th Legislature 1965) and Minute Order of Texas Highway Commission pursuant thereto dated February 16, 1966; Utah Code Ann. §§ 41–1–60 (Supp.1965), 41–1–61 (1953); Vt.Stat. Ann. tit. 23, § 109 (1959); Va.Code Ann. § 46.1–32 (1967); W.Va.Code Ann. § 1721 (140) (1961); Wis. Stat.Ann. § 341.17 (Supp.1967).

Defendant Polk, in an undisputed compilation of statutes which need not be reproduced here, reports its finding of provisions in every State except Kentucky making public records of vehicle registration information. The substantially uniform state practice is not decisive, but it is another item of some weight against plaintiff's constitutional theory. Cf. McGowan v. State of Maryland, 366 U.S. 420, 497, 81 S.Ct. 1153, 6 L.Ed.2d (1961) (opinion of Mr. Justice Frankfurter); Green v. Board of Elections, 380 F.2d 445 (2d Cir. 1967).

MEMORANDUM

JUNE 27, 1974.

Several letters have been sent to Senator Percy that provide examples of privacy invasions that involve mail advertisements and mail surveys.

Perhaps the most interesting example comes from Mr. Icenogle of Smithshire, Illinois. In his letter, Mr. Icenogle says that eight days after buying a new car he received an advertisement from the Fingerhut Corporation, makers of Air Flo seat covers, that indicated that they knew the make of his new car. The advertisement seems to indicate that they also knew something about Mr. Icenogle's occupation. He wonders how they got the information and he feels that his privacy has been invaded. I suspect, although I have no proof, that this company gets its information from the Department of Motor Vehicles in Illinois (this is a common practice in many states).

A second example comes from Trevanion H. E. Nesbitt of Bethesda, Maryland. Mr. Nesbitt received a subscription form letter from Newsweek magazine that was attached (at the bottom) to a subscriber survey. The survey asked for information about profession, job title, income and favorite charity of the respondent. Mr. Nesbitt feels that Newsweek has no business asking for this information. I think there is an additional problem in that Newsweek does not indicate exactly what the information will be used for. They claim that the charity will benefit from a contribution by Newsweek, but I suspect the

real benefit will be a mailing list which the charity can then use to solicit personal donations.

The third example comes from Robert Isbister of Las Vegas, New Mexico. He applied for insurance from State Farm Insurance Co. and two days later received a form from State Farm explaining that under the Fair Credit Reporting Act they were obliged to notify him of the fact that they had requested an Investigative Consumer Report on him from a credit investigation agency. The report would include information about his character, general reputation, personal characteristics, mode of living etc. that was gleaned from interviews with his friends and neighbors. Mr. Isbister objected to this practice because, he claims, he has had a member of the Mafia and a reputed drug dealer as neighbors and would not think them reliable witnesses as to his personal character.

FACT SHEETS

FEDERAL DATA BANKS

CONSTITUTIONAL RIGHTS SUBCOMMITTEE STUDY

In 1970, Senator Sam J. Ervin, Jr., ordered the staff of the Senate Constitutional Rights Subcommittee to conduct a survey of all Federal data banks and computers containing information on individual citizens. The results are contained in a summary report entitled: "Federal Data Banks and Constitutional Rights" issued on June 18, 1974.

The study took four years. The complete survey will be published in six volumes totalling over 4,000 pages when printed later this month. The conclusions are contained in a 53-page summary released today in connection with the opening of hearings on "Privacy, Computers, Data Banks and Government Information Systems" jointly held by the Constitutional Rights Subcommittee of the Judiciary Committee with an ad hoc Subcommittee of the Government Operations Committee.

The 54 executive branch agencies surveyed report a total of 858 data banks containing personal information about individuals.

Over 1¼ billion records on individuals are maintained in these systems, even though more than 10% of the data banks failed to state the number of records they contain.

Over 86% of these federal data banks are computerized.

Some data banks, like the decennial census, contain information on every citizen; others such as the Air Force Special Weapons Center Security File may be as small as ten subjects.

Some agencies have records with sensitive information on race, drug-addiction history, and salary but do not regard this as personal information.

Although most of the 54 agencies replying tried conscientiously to help the subcommittee in its work, many of the agencies replied slowly or only partially. Some agencies, like the Department of the Interior, failed to answer the survey at all. Others omitted significant data banks, or like General Services Administration, failed to report important new computer data bank plans.

Most data banks are said to be administrative in nature, but a significant number are used for evaluation and statistical purposes.

A relatively small number—about 29 data banks—are concerned primarily with derogatory information. These include agency blacklists, lookout files, intelligence, and civil disturbance files kept by such agencies as the Departments of Agriculture, Justice, Defense, and Treasury, Housing and Urban Development, as well as the Small Business Administration, and the General Services Administration. Most of these files are computerized.

The great majority of the surveyed data banks lack a specific statutory mandate. Most are created under general housekeeping authority, or as means of assisting authorized programs. Only 10% have been specifically authorized by statute.

Over 40% of the data banks do not tell citizens that records are kept on them. Another one-fourth of the responses state that they expect that citizens know about their data banks because they receive checks or other communications from the agency.

Only 30% expressly notify subjects; and at least one data bank uses a press release to do so.

About half of the data banks do not allow subjects to review or correct their files. Some of those which do allow file review do not inform citizens that files are kept on them. A handful require periodic review of files by subjects.

Over one-third of the data banks prohibit access by file subjects to their own records. Most, but not all of these, are intelligence files.

More than 60% of the data banks regularly share their files, or the information in them, with other agencies.

A small but surprising number—10 computer systems—allow regular computer-interface access by other agencies. These are mostly law enforcement systems like the Federal Bureau of Investigation's NCIC and the Department of the Treasury's TECS.

Some agencies distribute information to other parts of the government despite pledges of confidentiality. Internal Revenue Service and the Selective Service are among these.

In only a few cases do statutes specifically permit or require dissemination to other agencies or, conversely prohibit such access. The Driver Registry of the Department of Transportation and Agriculture's Commodity Exchange data bank share information with other agencies, in accordance with such express statutory directives.

Only a few data banks (11% of those surveyed) consider their files to be public information open to all. One data bank—the Civil Service Commission's List of Eligible Voters—is required by law to be public. However, most agencies stated that the Freedom of Information Act governs public access to their files.

Most agencies report the use of some type of security measures to safeguard their data banks. Of those that do take security measures, most rely only on physical security, such as locked rooms. A few agencies (5%) replied that they take no security precautions of any kind.

Only 15% of the files use electronic security devices of varying degrees of sophistication. However, because even some of the more sophisticated and sensitive data banks, such as the Treasury Department's TECS, have many remote terminals; unauthorized access or tapping into any one terminal will jeopardize the security of the entire data bank.

About 70% of the data banks derive their data from existing files and records. Almost as many use the subjects to supply some data; and about 40% go to outside third parties.

FEDNET

During 1973 GSA began work on a joint computer procurement to accommodate the needs of GSA and the Department of Agriculture. The System, FEDNET, is designed to consolidate and centralize the data processing and telecommunications operations of the two agencies, with modularity designed into the system so that it can be expanded indefinitely with the addition of other agencies. In short, a national data center approach.

The original joint request for bids (RFP) was issued on February 28, 1974. The proposal was for the procurement of up to 5 data centers for USDA and 4 for GSA, several thousand remote terminals throughout the country, and a GSA-operated telecommunications network. The proposal was to be funded through GSA's revolving ADP fund established by the Brooks Act in 1965. In this way, the FEDNET would not be subjected to congressional review or authorization. The fund is currently capitalized at $50 million.

However, after Congress and the Executive Branch became aware of the FEDNET program, opposition to it quickly mounted. OMB Director Roy Ash directed that the proposal be withdrawn on the grounds that the program was inconsistent with OTP guidance which had called for its termination; it lacked economic advantage; there were viable alternatives to the system; and it raised a potential threat to the right of privacy at a time when the Executive Branch and Congress are studying the issue. Vice President Ford in a speech before the National Computer Conference in Chicago expressed his concern that "Federal protection of individual privacy is not yet developed to the degree necessary to prevent FEDNET from being used to probe into the live of individuals."

In Congress, Representatives Moss, Moorhead and Roybal, and Senators Ervin, Hruska, Goldwater, Montoya and Eagleton all questioned the need for such a system, the desirability of such a system, and the manner in which the proposal was proceeding. The consensus was that such a system involved a policy decision which should not be made on an administrative level, but only by Congress after a thorough review of the system and its implications for privacy.

In response, Administrator Sampson agreed that the privacy concerns being raised were valid and that the issue was not fully considered before the proposal was released for bids. On May 16, he announced that the data communications

network would be deleted from the solicitation and procured separately, and that three of the four optional sites called for in the original solicitation would be deleted, and GSA's firm site would be made optional. Furthermore, as requested by Senator Montoya, the equipment procurement was delayed an additional four months so that Congress might have an opportunity to enact privacy legislation.

In terms of effect, Aministrator Sampson has not really addressed Congressional concerns. The program is proceeding, albeit somewhat delayed. The system design remains intact; the computer centers as well as the remote terminals will still be procured. The only significant change to the original concept is the deletion, temporarily, of the data communications network. When added at some future date, the original system will have been built, only in stages.

CHRONOLOGY

October 30, 1965. Brooks Act enacted (PL 89-306), amending the Federal Property and Administrative Services Act of 1949. This Act authorized and directed the Administrator of GSA to coordinate and provide for the economic and efficient purchase, lease and maintenance of automatic data processing equipment by federal agencies.

July, 1972. Office of Automatic Data Telecommunications Service (ADTS) established in GSA.

July, 1972. GSA began its plans to upgrade its federal data processing centers.

September 12, 1972. The Agricultural Stabilization and Conservation Service of USDA requested Air Force assistance in selecting automatic data processing equipment as part of Agriculture's plans to build departmental computer centers and establish a single departmental telecommunications network.

March, 1973. Agriculture adopted a plan for consolidating all USDA automatic data processing equipment and began working on technical specifications for ADP equipment for four major USDA computer centers with Air Force assistance.

April 12, 1973. USDA officials notified GSA by letter that it planned to release a request for proposal to industry and requested a delegation of procurement authority from GSA.

April 15, 1973. President Nixon's Executive Order 11717 transfers the policy control over automatic data processing to GSA from OMB; the functions relating to the establishment of government-wide autodata processing standards to the Secretary of Commerce. Oversight responsibilities remain with OMB.

May, 1973. Discussions were held between USDA and GSA to determine the feasibility of combining the two sets of requirements.

June 26, 1973. Representatives of GSA testified before the House Subcommittee on Foreign Operations and Government Information on Federal Information Systems and plans without mentioning their plans for FEDNET.

July, 1973. GSA and USDA joined in a combined effort to procure large scale computer centers. GSA included its concept of a data communications network in the specifications.

December, 1973. GSA advertised the joint bid proposal in the Commerce Business daily.

January–February, 1974. Source Selection Board established consisting of representatives from USDA, GSA and Air Force. The Board has the responsibility for recommending the equipment supplies as a result of the competitive selection process.

February, 1974. Social Security Administration briefed on FEDNET.

February 28, 1974. Request for proposal for FEDNET released to industry.

March, 1974. GSA informally briefed the Bureau of Customs on FEDNET.

April, 1974. Veterans Administration briefed by GSA on FEDNET.

April 25, 1974. Congressman Moss wrote GSA inquiry about FEDNET.

April 30, 1974. OTP director Clay Whitehead wrote GSA of his concern over the approach GSA is taking to obtain data processing and communications network services.

May 6, 1974. Senator Ervin, Senator Hruska, and Senator Goldwater wrote GSA expressing concern about FEDNET.

May 7, 1974. A separate USDA Request for Proposal (ADS-74-5-512) was issued for up to 4300 remote terminals to support FEDNET.

May 9, 1974. Vice-President Ford expressed his concern over FEDNET in a speech before the National Computer Conference in Chicago.

May 9, 1974. OMB Director Roy Ash wrote GSA that its proposal to acquire 9 computer sites and a data communications network should be withdrawn.

May 14, 1974. House Appropriation Subcommittee hearings where for the first time GSA publicly answered congressional questions about FEDNET.

May 16, 1974. GSA notified bidders that an amended RFP would be issued in approximately 60 days. The RFP would reduce the number of ADP sites and eliminate the communications network from the procurement.

May 22, 1974. A GAO study of FEDNET was requested by Congressman Moss and Senator Ervin.

May 24, 1974. GSA Administrator Sampson officially notified Congressman Moss and Senator Ervin that the procurement proposal would be amended to reduce the number of ADP sites and delay the communications network for one year until privacy safeguards would be considered.

May 30, 1974. Senate Appropriation Hearing at which Senator Eagleton moved that appropriate language be placed in GSA's appropriation to prohibit the establishment of FEDNET or any similar system until Congress has reviewed and authorized the system. Chairman Montoya requested a 4 month delay in the proposal until Congress could review it.

June 5, 1974. GSA Administrator Sampson wrote Senator Montoya agreeing to a 4 month delay in awarding the FEDNET contract. However work on the proposal will continue. The data communications network will be deleted from the RFP and procured separately in about 12 months.

INDIVIDUAL CASES ILLUSTRATING NEED FOR THE NEW LAW

STAFF REPORT TO THE SENATE SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS, NOVEMBER 1973

PRIVACY: THE RIGHT TO SEE ONE'S OWN FILE

One aspect of the Subcommittee's study of the manner in which information is collected, maintained and disseminated in the federal government is the right of an applicant for federal employment to knowledge of his files. In this regard the Subcommittee intervened in the case of a woman who was refused a personal interview by the Air Force in order for her to confront and refute certain derogatory information which had been made part of her investigatory file and used to deny her a position for which she had applied.

After a year-long effort by the Subcommittee and Senator Ervin the Air Force finally granted the woman the interview, informed her of the nature and substance of the information it had compiled, and permitted her an opportunity to comment on the information.

Encouraged by the Air Force's action, Senator Ervin remarked that the decision "goes a long way toward recognizing the basic due process rights of applicants contained in Air Force regulation 40–732."

The case involved a temporary-hire clerical employee of the Air Force who had applied for a permanent position and was denied that position on the basis of derogatory information compiled during a routine background investigation. The Air Force maintained that, prior to the conclusion of this investigation, *substantial unfavorable criminal information was confirmed* about her. While she was not prosecuted for these activities, their nature was such that she would not be suitable for sensitive AFOSI employment. Based upon this information, further investigation was terminated and her supervisor was advised that she was unsuitable for AFOSI employment. (Emphasis added).

This accusation came as a shock to the applicant who wrote the Subcommittee that she had "absolutely no idea of what the denial could have been based upon." She has no criminal record and has never been detained, held, arrested, indicted or summoned into court as a defendant in a criminal proceeding.

The Air Force subsequently attempted to clarify their characterization of the unfavorable information.

"We regret any confusion that may have resulted from the statement in our previous letter to you that 'substantial unfavorable criminal information was confirmed' about [the woman]. These terms were not intended to imply that the Air Force considers [the woman] a criminal, but were used only to describe unfavorable information that was obtained from more than one source. . . . These terms are 'terms of art' in the investigative community but should not have been used in external correspondence."

Despite the seriousness of the accusations, the applicant was continually denied the right to pursue her case according to Air Force procedures. Completely frustrated in her attempts to find out what was in her file, the applicant turned to the Subcommittee for help.

As a result of continued Subcommittee inquiry, the Air Force conceded informally that on the basis of the information obtained there was no substance to the conclusion that the applicant was personally engaged in unsuitable conduct, much less "confirmed criminal" activity. In fact, the information primarily related to the activities and associations of her former husband. That marriage has been annulled and the woman had since remarried. The Air Force in effect conceded the error when it offered the applicant "the opportunity to interview for another position at [the base]." Nevertheless, they persisted in refusing her an opportunity to confront the charges.

In its negotiations with the Subcommittee the Air Force attempted to take refuge in strained interpretations of the applicant's status. They contended that the woman was a temporary employee and as such "had no employment rights". However, the Subcommittee strenuously disagreed with that interpretation of the woman's status. Maintaining that the procedural rights the applicant sought were in connection with the permanent position for which she had applied and not her temporary position, the Subcommittee argued that the woman was entitled to the full panoply of rights accorded all applicants for permanent position under the Air Force regulations.

Finally the Air Force wrote that although it did not agree with the Subcommittee's interpretation, it was prepared to "destroy [the applicant's] background investigation file, together with all other materials relating to the partial investigation." In the alternative, with the subject's permission, "the background investigation could be completed which would include a personal interview. At about that time she would be advised of the nature of the allegations made by various persons and would be given an opportunity to comment upon them."

In response to this offer, and after consultation with the applicant, Senator Ervin wrote:

"At the outset let me reiterate that my interest in this case is to protect the procedural and constitutional rights of individuals, and not to second guess the Air Force on its selection of any particular employee. I appreciate that the Air Force has established criteria and standards which prospective employees must meet and, of necessity, that these criteria are more stringent in OSI. However, apart from any employment criteria, basic procedural safeguards must be available to all applicants to insure against the possibility that they may be unjustly rejected or "nonselected" for a position. It is those procedures to which I am addressing myself in this case.

"Obviously, the offer to destroy the investigative file will not resolve the controversy. Throughout this matter what [the applicant] has continually sought is to be informed of the nature and substance of the unfavorable information OSI developed during her full field background investigation, and be permitted an opportunity to refute the allegations.

"Although that opportunity is offered in your alternative solution, the condition which is imposed before an interview can be granted is, in my opinion, unjustified. I see no necessity for completing the abandoned investigation simply to inform [the subject] of the facts the Air Force has already collected and acted upon. Nothing in Air Force regulations requires that the subject interview be the last investigative act taken and I perceive no reason why the Air Force cannot grant [the subject] an interview at this time without reopening the investigation.

On September 13, 1973, the Air Force responded.

"[I]n consonance with your request, arrangements are now under way to afford [the applicant] an interview. She will be apprised of the nature and substance of the derogatory information and given the opportunity to comment. The interview will be conducted by a senior Air Force Office of Special Investigations representative as soon as practicable."

The interview was held on September 12.

This case vividly points up the need to guarantee individuals the right of access to records containing personal information in order to correct misleading or incorrect information.

In summing up the interview in a letter to Senator Ervin, the woman wrote,

"I am truly sorry that these people think this way of me simply because I was married to ———. . . . I feel that the two agents who sat in on the interview believed that I was unaware of all that [he] was involved in and that if I had been aware, I certainly would not have condoned any of it, as they were led to believe I did."

CENSUS QUESTIONNAIRE

AUGUST 21, 1974.

HON. SAM J. ERVIN, JR.,
U.S. Senate, Committee on Government Operations,
Washington, D.C.

DEAR SENATOR ERVIN: I sincerely appreciate this opportunity to personally respond to your request for information about my experience and knowledge of the governments invasion of my "personal right to privacy". I will address my remarks to the Committee on Government Operations now studying the estab-

lishment of a *Privacy Protection Commission* and your enclosed confidential committee report.

To my knowledge, I was the only one of millions of Americans prosecuted, convicted and fined in Federal Court for refusing to answer certain questions on the D–2 long form of the U.S. Census Bureau issued at *random* to approximately 15% of the American public.

To absolutely clarify my reason, I objected *not to the collection of information*, but to the governments threat of a jail sentence and fine concerning the questions not related to the constitutional issue of counting heads for fair represenation in the U.S. Congress.

I am not a philosophical nut or of any particular ideological persuasion either to the right or the left, I'm just an average representative (in the past) of thousands of average Americans who genuinely and rightfully object to religious, financial, political and intimate personal questions stated in the mandatory D–2 long form. I tried various means to bring this issue to public and then political attention for three years preceding the 1970 census by sponsoring House resolutions, sending letters to Congress and introducing resolutions for adoption by local and national political platforms.

On April 1, 1970, I filled in all the questions necessary and required by the Census Bureau and left blank all the incidental questions. I wrote "none of your business" across each blank page and promptly mailed my form.

The first response from the government was through the U.S. Attorney's office. The U.S. Attorney called me through our Governor's office while the legislature was in session and threatened to prosecute me unless I filled in the additional questions left blank—I refused and said "prosecute away."

The second response was through the Governor's office from the Governor, political financiers and party leaders. They tried to persuade me to fill in the form or face certain prosecution which would be embarrassing for the national administration. My response was to offer my resignation both from the party and the legislature, but I refused to be intimidated.

The next response was reports that part-time census personnel were interviewing my neighbors and professional colleagues regarding personal information about myself and my family—I again refused.

As a college instructor at Wilmington College, my students were interviewed and my class record was investigated to find out if I were some type of subversive preaching against our government. Would you believe, an ex-marine judo drill instructor, graduate from a State College on the G.I. Bill, YMCA Director, public school and college instructor and republican state legislator is un-American.

Finally, I was then served with a subpoena and informed of the charges of violations of the Census Law. I was again offered the opportunity to fill in the blanks—I refused.

My attorney, Lawrence M. Sullivan, twice had the governments charge thrown out of Court and the third time it was brought to trial. This trial ended with a hung jury and I was tried a fourth time.

During all this time I was harassed both politically and personally by census personnel and my case was talked about freely both publicly and in the census office.

I was eventually convicted, fined $100.00 and given a 60-day probation during which time I was instructed by the judge to fill in the D–2 form. The end result was that the Census Bureau was protected to use the same tactics in 1980 on unsuspecting Americans.

My personal life became a series of harassment. I was ridiculed and humiliated by the local press as somewhat un-American, and certainly immature for not trusting the government. Personal friends, political and professional associates avoided me in an embarrassed manner. It damaged my political credibility and brought my business career almost to a halt. Editorial writers were delighted to have someone to crusade against and Mr. Stans, then Secretary of Commerce, stated I should be jailed. Since these events, I dropped out of politics, was forced to reorganize my business and entered Law School. But if given the opportunity, I would do it all again—*this time with vigor*!! When you are right, you have time on your side.

Few Delawareans stood up to be counted publicly on my behalf. Mr. Sullivan, assisted by Francis Paintin, worked extremely hard to win the issue and never sent a bill. Senator William V. Roth, now a member of your Committee, then in the House of Representatives, spoke up on my behalf and successfully fought

for this issue in the Congress. Mr. Henry Topel, then Democratic State Chairman, complimented me publicly and refused to make it a partisan issue.

I thank these men who are dedicated to the American constitutional right to privacy and I sincerely thank you and your committee for your absolute dedication on behalf of all Americans as the recent tragic events prove out your case for the public.

Respectfully yours,

THOMAS L. LITTLE.

[From the Delaware State News, Dover, Del., October 10, 1971]

EVEN OPPONENTS LIKE HIM A LITTLE

WILMINGTON—"When I make a commitment, I make it really firm. I put my head down and go—some say this is a failing in me."

Tom Little does not believe in doing things halfway. The state representative from Deerhurst has achieved both fame and notoriety for this characteristic.

He committed himself to bucking the Census Bureau last year and it took an order from a judge to get his signature on the form.

"I'm a perfect Aquarian, fiercely independent. The challenge is the thing for me—I enjoy the battle more than the winning. And I love campaigns.

"I've raised myself since I was 13, and I've had to be independent. So I really don't see why I should kowtow to institutional families and establishments now."

Loyalty is one of the subsections under Tom's commitment heading. "I'm one of those people who stands by until the end. When everybody else is deserting the ship, I'm the one who sticks with it. It's one of my characteristics that I'm proud of."

An acquaintance says Tom is "almost fantastically loyal as a friend. And he expects the same loyalty from you."

Tom, now 35, has handled some big responsibilities since his teen years. At 19. he was a drill instructor in the Marine Corps, and at 20 he developed a judo program for the entire corps.

He worked his way through Bloomsburg (Pa.) State College as a bartender on the 6 p.m.-to-2 a.m. shift. He played varsity football, was captain of the swimming team, and still managed to get his degree in three years.

Tom came to Delaware as a swimming coach. "I loved coaching. I ate, slept and drank swimming. I loved it and quit it.

"I could quit politics, too.

"I'm at a crossroads right now. I don't know if I want to be an educator, a businessman, a lawyer or a politician."

(Tom has enrolled in Delaware's new law school, just in case things work out that way.)

There is much speculation concerning Tom's political future, and he's speculating as much as anyone. "I couldn't see myself as governor, though. I wouldn't like an administrative job—I want to be in there where the action is. Maybe in national politics."

Tom has one ambition that seems a little out-of-character to those who know him for his exuberance. "If I could get rid of all this energy, I'd like to write. I like ideas, like to think things out."

He's made a start in this direction already, with seven chapters written for a book to be titled *Me and Sam Muldoon.*

A firm belief in fair play is another of Tom's characteristics. "I play a fair game in everything I do. I have a personal philosophy of always giving more than I ask for, so I'm always one up.

"I give a lot of consideration before I make a commitment, because I know I'm going to have to abide by it. But when I make the commitment, whether it be in a political campaign, football or judo, I go straight for the throat.

"Sombody once said I have a jugular instinct."

"But when you make this strong a commitment, you have to expect to get hurt. When you challenge someone or decide to attack, you have to realize that you yourself can be destroyed."

Even Tom's political opponents uphold his claim to fair play. His first opponent says, "If I ever ran again, I couldn't find a nicer guy to run against. He's completely ethical and upright.

"I couldn't say a single thing against Tom, except that he's a Republican."

Other persons who know Tom were contacted for opinions, but words like "terrific," "great," and "fantastic," came up so often that the effort was abandoned for lack of originality.

Tom says he has a knack of doing things in an unorthodox manner. "I don't get up in the morning and say 'what can I do different today?' It just happens that I don't always do things the way other people do them."

A case in point concerns his son Patrick. "I had him put in jail for stealing when he was four. I got all kinds of terrible letters and calls from the mothers in the neighborhood, but I haven't seen him steal anything else, and he has a healthy respect for jails."

Apparently Patrick, now 8, is following in his father's footsteps as an independent thinker. "I told him to quit bugging me about a raise in his allowance and go get a job. So he did.

"He took my neckties around the neighborhood and sold them for a quarter each. It was fantastic!"

Tom and his wife Kay have two other children, Ann, 9, and Kelly, who will be five this week.

Tom has a reputation for having a "teriffic relationship with his kids," as one acquaintance put it. "He chases his wife and the girls away and he and Patrick watch "The Courtship of Eddie's Father" alone, just the two of them. He really relates to his kids better than most parents."

WILLIAM E. PARVIS
CHIEF U. S. PROBATION OFFICER
EUGENE A. MAYHEW
U. S. PROBATION OFFICER

U. S. COURT HOUSE
WILMINGTON 19801
658-6911-EXT. 249
FTS 302-658-6349

UNITED STATES DISTRICT COURT

OFFICE OF THE PROBATION OFFICER
DISTRICT OF DELAWARE

October 1, 1971

Mr. Thomas L. Little
16 York Road
Wilmington, Delaware 19803

Dear Mr. Little:

Clearance with the Clerk of the United States District Court, District of Delaware, reveals that the $100.00 fine imposed as part of your sentence is still outstanding.

Your probationary period is due to expire on October 8th, 1971 and the $100.00 fine is to be paid in full by that date. A money order or certified check should be made payable to "Clerk, U. S. District Court, District of Delaware."

If you have any questions regarding this letter, do not hesitate to contact me.

Very truly yours,

William E. Parvis

William E. Parvis
Chief U. S. Probation Officer

WEP:ls
Enc. (Monthly Supervision Report)

FEDERAL PROBATION AND PAROLE FORM A (FEB 70)

MONTHLY SUPERVISION REPORT

REPORT FOR MONTH OF: SEP 1971

CHECK TYPE OF SUPERVISION: PAROLE; MANDATORY RELEASE; MILITARY PAROLE; DEFERRED PROSECUTION; PROBATION

INSTRUCTIONS

Submit this report to the Probation Office as directed.

Return by October 8, 1971

FULL NAME (print or type)

REGISTER NUMBER (if any) | TELEPHONE NUMBER (if any)

ADDRESS | MAIL ADDRESS

Zip Code | Zip Code

DID YOU MOVE DURING THE MONTH? ☐ YES ☐ NO | IF YOU HAVE MOVED, EXPLAIN WHY

NAME AND ADDRESS OF YOUR EMPLOYER (or school) | IF EMPLOYED, WHAT IS YOUR JOB?

HAVE YOU CHANGED JOBS DURING THE MONTH? ☐ YES ☐ NO | WHAT WAS THE TOTAL AMOUNT YOU EARNED FROM EMPLOYMENT DURING THE MONTH BEFORE DEDUCTIONS? | HOW MANY DAYS DID YOU WORK (or attend school) DURING THE MONTH?

IF YOU ARE NOT WORKING, OR HAVE CHANGED JOBS, EXPLAIN WHY

DID YOU RECEIVE ANY MONEY OTHER THAN FROM EMPLOYMENT SUCH AS LOANS, RELIEF BENEFITS, ETC? ☐ YES ☐ NO | IF SO, GIVE AMOUNTS AND FROM WHOM RECEIVED

DO YOU HAVE ANY DEBTS WHICH ARE PAST DUE? ☐ YES ☐ NO | IF SO, GIVE AMOUNTS AND TO WHOM OWED

WERE YOU ARRESTED DURING THE MONTH? ☐ YES ☐ NO | IF SO, GIVE DATE OF ARREST | PLACE OF ARREST

WITH WHAT OFFENSE WERE YOU CHARGED? (explain) | DISPOSITION MADE (fine, jail, dismissed, etc.)

REMARKS, INCLUDING EXPLANATION OF ARRESTS, IF ANY (use reverse side for additional space)

SIGN HERE ⇨ _____ DATE ⇨ _____

DO NOT WRITE BELOW THIS LINE

ADVISER'S COMMENTS:

I have seen the above named personally _____ times during the month.

SIGNATURE OF ADVISER _____ DATE _____

PROBATION OFFICER'S COMMENTS:

SIGNATURE OF PROBATION OFFICER _____ DATE _____

RETURN THIS REPORT TO:

William E. Parvis, Chief
U. S. Probation Officer
349 Federal Building
Wilmington, Delaware 19801

FPI MI—2-9-70-500-M-4496

PRESS CONFERENCE STATEMENT BY TOM LITTLE AFTER CONVICTION TO POLITICAL LEADERS IN THE 11TH DISTRICT OF DELAWARE

Three years ago I became involved in trying to encourage Congress to make certain intimate questions during the 1970 Census voluntary. I co-sponsored a resolution with Neal Moerschel which was sent to our Congressional Delegation very soon after I was elected. The resolution asked that the United State Congress remove the jail penalty and fine for certain questions considered not pertinent to the actual enumeration of the population.

In July, 1969, as part of my national campaign for Treasurer of the Young Republicans—this was a major issue. I was successful in having it adopted as a plank in our national platform. It was adopted by the entire Convention. Previous attempts to solve this problem has been unsuccessful although even the major political leaders stood strong behind this issue including Bill Roth and Richard Nixon. The problem was not resolved by April 1, 1970. Since I have extensive involvement and the Census only occurs every ten years, I felt the moral obligation to test the law in the courts. Some people call it courage; some people call it stupid. I recognize the pitfalls. However, there is a significant minority of people in this country that I felt obligated to, despite the potential backlash, that I should follow through. There are 8 million people at this time who have not filled in their Census form; there are many millions who have singled out certain questions to not answer; there are even many more millions who filled it in begrudgingly. I knew that as a private citizen the Census Bureau would ignore me completely as they have the millions of others. However, I also knew as a public official they would have to act in my case to justify their existence. This is why I made the decision. The political threat and the erosion of public image have been significant enough to cause me to try to look more objectively at my action. However, it's difficult because I am so committed to the principle of individual freedom that I need outside advice.

Hope this provides some explanation to my stand on the United States Census.

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Criminal Action No. 2054
	)	
THOMAS L. LITTLE,	)	1970
	)	
Defendant.	)	

PLAINTIFF'S OPENING BRIEF IN
SUPPORT OF HIS MOTION TO DISMISS

LAWRENCE M. SULLIVAN
Sullivan, Potter & Roeberg
1112 King Street
Wilmington, Delaware
Attorney for the Defendant

TABLE OF CONTENTS

	PAGE
CASES CITED	ii, iii
AUTHORITIES	iv
STATEMENT OF FACTS AND NATURE OF THE PROCEEDINGS	v
ARGUMENT I THE INFORMATION FAILS TO STATE FACTS SUFFICIENT TO CONSTITUTE AN OFFENSE AGAINST THE UNITED STATES	1-2
ARGUMENT II THE INFORMATION FAILS TO ADEQUATELY INFORM THE DEFENDANT OF THE NATURE OF THE CHARGE AGAINST HIM IN VIOLATION OF THE DEFENDANT'S RIGHTS GUARANTEED BY THE UNITED STATES CONSTITUTION	3-6
ARGUMENT III THE STATUTE UPON WHICH THE CHARGE IS BASED, I.E. TITLE 13 UNITED STATES CODE, SECTION 221(a) IS UNCONSTITUTIONAL IN THAT IT IS VAGUE AND INDEFINITE	7-9
ARGUMENT IV THE DELEGATION OF POWER BY THE UNITED STATES CONGRESS TO THE SECRETARY OF COMMERCE AS EXPRESSED IN TITLE 13, UNITED STATES CODE, CHAPTER V, IS UNCONSTITUTIONAL IN THAT IT LACKS AN INTELLIGIBLE STANDARD TO WHICH ADMINISTRATIVE ACTION MUST CONFORM	10-14
ARGUMENT V THE EXERCISE OF POWER BY THE SECRETARY OF COMMERCE CONSTITUTED AN INVASION OF THE DEFENDANT'S CONSTITUTIONAL RIGHT TO PRIVACY	15-17
CONCLUSION	18

TABLE OF CASES

	PAGE
Cochran and Sayre v. United States, 157 U.S. 286, 15 S.Ct. 628, 39 L.Ed. 704	3
Connolly v. General Construction Co., 269 U.S. 385, 391, 46 S.Ct. 126, 127, 70 L.Ed. 322	8
Hagner v. United States, 285 U.S. 427, 431, 52 S.Ct. 417, 419, 76 L.Ed. 861	3
Harriman v. Interstate Commerce Commission, 211 U.S. 407, 29 S.Ct. 115, 117, 53 L.Ed. 253	12
Interstate Commerce Commission v. Brimson, 154 U.S. 447, 14 S.Ct. 1125, 38 L.Ed. 1047	16
Johnson v. Boeing Airplane Co., 262 P.2d 808	15
Kilbourn v. Thompson, 103 U.S. 168, 195, 26 L.Ed. 377	13, 15, 16
Lanzetta v. New Jersey, 306 U.S. 451, 453, 59 S. Ct. 618, 619, 83 L.Ed. 888	8
McBoyle v. U.S., 283 U.S. 25, 51 S.Ct. 34	9
McGrain v. Dougherty, 273 U.S. 135, 183, 47 S.Ct. 319, 328, 71 L.Ed. 580	15
In re Pacific Railway Commission (Circuit Ct., N.D. Cal.) 32 F. 241	16
Rosen v. United States, 161 U.S. 29, 16 S.Ct. 434 40 L.Ed. 606	3
Russell v. United States (1962) 369 U.S. 749, 82 S.Ct. 1038	2, 4, 5
Sunshine Cool Co. v. Adkins, 310 U.S. 381, 398 (1940)	13
United States vs. Selah C. Carll (1892) 105 U.S. 611 26 S.Ct. 1135	1
United States v. Cruikshank, 92 U.S. 542, 558, 23 L.Ed. 588	3

United States v. Harriss, 347 U.S. 612, 74 S.Ct. 808, 812, 98 L.Ed. 989 — 8

United States v. Hess, 124 U.S. 483, 487, 8 S.Ct. 571, 573, 31 L.Ed. 51(b) — 4

United States v. L. Cohen Grocery Co. (1921) 255 U.S. 81 — 9

AUTHORITIES

	PAGE
Title 13 U.S.C. §221	2, 5, 7, 11
Title 13 U.S.C. Chapter 5	10, 11, 12
Title 13 U.S.C.A.	7
Title 13 U.S.C.A. Chapter 5	7
Title 13 U.S.C.A. Chapter 7	7
2 U.S.C. §192	4, 5
2 U.S.C.A. §192	4, 5

STATEMENT OF FACTS AND NATURE OF THE PROCEEDINGS

The defendant, Thomas L. Little, has been charged with violating Title 13, United States Code, Section 221(a) by an information dated June 19, 1970 and signed by F. L. Peter Stone, United States Attorney for the District of Delaware.

On June 19, 1970, the defendant voluntarily appeared before the Honorable Edward J. Pollard, United States Commissioner and was released on his own recognizance.

On July 2, 1970, the defendant was arraigned before the Honorable Caleb Layton, Senior Judge of the United States District Court for the District of Delaware. The defendant entered a plea of not guilty.

On July 13, 1970, defendant filed a Motion to Dismiss the information and a Motion for a Bill of Particulars. On July 30, 1970, the United States filed an answer to the Defendant's Motion for a Bill of Particulars.

This brief is offered in support of the defendant's Motion to Dismiss the information.

ARGUMENT I

THE INFORMATION FAILS TO STATE FACTS SUFFICIENT TO CONSTITUTE AN OFFENSE AGAINST THE UNITED STATES

The Supreme Court of the United States in United States vs. Selah C. Carll (1882) 105 U.S. 611, 26 S.Ct. 1135 has held that where the elements of the crime have to be ascertained by reference to the common law or to other statutes, it is not sufficient to set forth the words of the statute. Mr. Justice Gray delivered the opinion of the court:

> "In an indictment upon a statute, it is not sufficient to set forth the offense in the words of the statute, unless those words of themselves fully, directly and expressly, without any uncertainty or ambiguity, set forth all the elements necessary to constitute the offense intended to be punished; and the fact that the statute in question, read in the light of the common law, and of other statutes on the like matter, enables the court to infer the intent of the Legislature does not dispense with the necessity of alleging in the indictment all the facts necessary to bring the case within that intent. U. S. v. Cruikshank, 92 U.S. 542 [XXIII., 588]; U.S. v. Simmons, 96 U.S. 360 [XXIV., 819]; ... The omission is a matter of substance, and not a 'defect or imperfection in matter of form only,' within the meaning of section 1025 of the Revised Statutes. By the settled rules of criminal pleadings, and the authorities above cited, therefore, the question of the sufficiency of the indictment must be answered in the negative."

More recently in Russell v. United States (1962) 369 U.S. 749, 82 S.Ct. 1038, the Supreme Court held that certain indictments charging the defendant's refusal to answer certain questions when summoned before a congressional subcommittee were insufficient where they did not identify the subject under inquiry at the time of the defendant's alleged default or refusal to answer. In that case Mr. Justice Steward delivered the opinion of the court which said, inter alia:

> "...the very core of criminality under 2 U.S.C. §192, 2 U.S.C.A. §192 is pertinency to the subject under inquiry of the questions which the defendant refused to answer. What the subject actually was, therefore, is central to every prosecution under the statute. Where guilt depends so crucially upon such a specific identification of fact our cases have uniformly held that an indictment must do more than simply repeat the language of the criminal statute."

In the case at bar, it is crucial to know the specific questions which the defendant is alleged to have "refused and wilfully neglected to answer" in order to determine whether they are "applicable to the [defendant] and his family" as required by Title 13, United States Code, Section 221(a). It is also crucial to know the pertinence of such questions to the purpose of the census.

In view of the fact that neither the specific questions nor their pertinence have been alleged, the information fails to state facts sufficient to constitute an offense against the United States.

ARGUMENT II

THE INFORMATION FAILS TO ADEQUATELY INFORM THE DEFENDANT OF THE NATURE OF THE CHARGE AGAINST HIM IN VIOLATION OF THE DEFENDANT'S RIGHTS GUARANTEED BY THE UNITED STATES CONSTITUTION

The Sixth Amendment of the United States Constitution provides that "In all criminal prosecutions the accused shall enjoy the right ... to be informed of the nature and cause of the accusation; ..."

The Supreme Court has, in a number of cases, emphasized the protections which informations and indictments are intended to guarantee. Two criteria have been advanced by which the sufficiency of the information or indictment is to be measured. The criteria are, first, whether the information or indictment "... contains the elements of the offense intended to be charged, and sufficiently appraises the defendant of what he must be prepared to meet;" and secondly, "... in case any other proceedings are taken against him for a similar offense whether the record shows with accuracy to what extent he may plead a formal acquittal or conviction." Cochran and Sayre v. United States, 157 U.S. 286, 15 S.Ct. 628, 39 L.Ed. 704; Rosen v. United States, 161 U.S. 29, 16 S.Ct. 434, 40 L.Ed. 606, Hagner v. United States, 285 U.S. 427, 431, 52 S.Ct. 417, 419, 76 L.Ed. 861.

In United States v. Cruikshank, 92 U.S. 542, 558, 23 L.Ed. 588 the court said:

> "It is an elementary principle of criminal pleading that where the definition of an offense, whether it be a common law or by statute, 'includes generic terms, it is not sufficient that the indictment shall charge the offense in the same generic terms as in the definition; but it must state the species, -- it must descend to particulars.'"

Furthermore, in United States v. Simmons, 96 U.S. 360 at page 362, 24 L.Ed. 819, it was said that an indictment which was not drafted to inform the defendant "with reasonable certainty, of the nature of the accusation against him ... is defective although it may follow the language of the statute."

And in United States v. Hess, 124 U.S. 483, 487, 8 S.Ct. 571, 573, 31 L.Ed. 51(b), the court said:

> "Undoubtedly, the language of the statute may be used in the general description of an offense, but it must be accompanied with such a statement of the facts and circumstances as will inform the accused of the specific offenses coming under the general description, with which he is charged."

Russell v. United States (1962) 369 U.S. 768, 82 S.Ct. 1038 is a case which is closely parallel to the case at bar. In Russell, a series of defendants were indicted for refusing to answer questions posed by a congressional subcommittee. The defendants were charged with violating 2 U.S.C. §192, 2 U.S.C.A. §192, a statute which is quite similar to the statute under which the present defendant is charged. The former statute reads as follows:

> "Every person who having been summoned as a witness by the authority of either House of Congress to give testimony or to produce papers upon any matter under inquiry before either House or any joint committee established by a joint or concurrent resolution of the two Houses of Congress, or any committee of either House of Congress, wilfully makes default, or who, having appeared, refuses to answer any question pertinent to the question under inquiry, shall be deemed guilty of a misdemeanor, punishable by a fine of not more than $1,000 nor less than $100 and imprisonment in a common jail for not less than one month nor more than twelve months" 2 U.S.C. §192, 2 U.S.C.A. §192.

The statute under which the present defendant is charged reads as follows:

> "Whoever, being over eighteen years of age, refuses or wilfully neglects, when requested by the Secretary, or by any other authorized officer or employee of the Department of Commerce or bureau or agency thereof acting under the instructions of the Secretary or authorized officer, to answer, to the best of his knowledge, any of the questions on any schedule submitted to him in connection with any census or survey provided for by subchapters I, II, and IV of Chapter 5 of this title, applying to himself or to the family to which he belongs or is related, or to the farm or farms of which he or his family is the occupant, shall be fined not more than $100 or imprisoned not more than sixty days, or both." 13 U.S.C. §221(a)

The Supreme Court, in Russell, reversed the decision of the Court of Appeals which had denied the defendants' motion to quash the indictments. The court said the indictments were insufficient for they failed to identify the subject which was under inquiry at the time of the defendants' alleged default or refusal to answer.

The Court went on to say:

> "The vice which inheres is the failure of an indictment under 2 U.S.C. §192, 2 U.S.C.A. §192 to identify the subject under inquiry is thus the violation of the basic principle 'that the accused must be apprised by the indictment, with reasonable certainty, of the nature of the accusation against him, ...' United States v. Simmons, supra, 96 U.S. at 362. A cryptic form of indictment in cases of this kind requires the defendant to go to trial with the chief issue undefined. It enables his conviction to rest on one point and the affirmance of the conviction to rest on another. It gives the prosecution free hand on appeal to fill in the gaps of proof by surmise or conjecture."

Due to the fact that the information fails to list the specific questions the defendant is alleged to have neglected or wilfully refused to answer, and further due to the fact that the pertinence of those questions has not been alleged therein, the defendant has been inadequately informed as to the nature of the charge against him.

37-583 O - 74 - pt. 2 - 61

ARGUMENT III

THE STATUTE UPON WHICH THE CHARGE IS BASED, I.E. TITLE 13 UNITED STATES CODE, SECTION 221(a) IS UNCONSTITUTIONAL IN THAT IT IS VAGUE AND INDEFINITE

In the instant case the statute upon which the charge is based is Title 13, United States Code, Section 221(a). It reads as follows:

> "Whoever, being over eighteen years of age, refuses or wilfully neglects, when requested by the Secretary, or by any other authorized officer or employee of the Department of Commerce or bureau or agency thereof acting under the instructions of the Secretary or authorized officer, to answer, to the best of his knowledge, any of the questions on any schedule submitted to him in connection with any census or survey provided for by subchapters I, II, and IV of Chapter 5 of this title, applying to himself or to the family to which he belongs or is related, or to the farm or farms of which he or his family is the occupant shall be fined not more than $100 or imprisonment not more than sixty days, or both."

In order for a person to know whether he has violated the statute above, he would, of necessity, have to know the provisions of subchapters I, II, and IV of Chapter 5 of Title 13 U.S.C.A. as well as subchapter 225 of Chapter 7 of Title 13 U.S.C.A. The latter statute is even more vague than Section 221(a). It states the applicability of penal provisions in certain cases.

The Supreme Court of the United States has often recognized the basic principle that a criminal statute must give fair warning of the conduct that it makes a crime. In the case of United States v. Harriss, 347 U.S. 612, 617, 74 S.Ct. 808, 812, 98 L.Ed. 989, the court said:

> "The constitutional requirement of definiteness is violated by a criminal statute that fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute. The underlying principle is that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed."

In Connolly v. General Construction Co., 269 U.S. 385, 391 46 S.Ct. 126, 127, 70 L.Ed. 322, the court struck down a state criminal statute under the Due Process Clause where it was not "sufficiently explicit to inform those who were subject to it what conduct on their part would render them liable to its penalties." The court went on to say:

> "A statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates the first essential of due process of law."

In the case of Lanzetta v. New Jersey, 306 U.S. 451, 453, 59 S.Ct. 618, 619, 83 L.Ed. 888, Justice Butler wrote:

> "It is the statute, not the accusation under it, that prescribes the rule to govern conduct and warns against transgression. See Stromberg v. California 283 U.S. 359, 368, 51 S.Ct. 532, 535, 75 L.Ed. 1117, 73 A.L.R. 1484; Levell v. Griffin, 303 U.S. 444, 58 S.Ct. 666, 82 L.Ed. 949. No one may be required at peril of life, liberty or property to speculate as to the message of penal statutes. All are entitled to be informed as to what the State commands or forbids."

Mr. Justice Oliver Wendell Holmes delivered the opinion of the court in McBoyle v. U. S., 283 U.S. 25, 51 S.Ct. 34, wherein it was said, inter alia:

> "Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear..."

The defendant in the present case contends that the statute which charges him "lacks an ascertainable standard of guilt" and is not "adequate to inform persons accused of violations thereof of the nature and cause of the accusations against them." See United States v. L. Cohen Grocery Co. (1921) 255 U.S. 81.

ARGUMENT IV

THE DELEGATION OF POWER BY THE UNITED STATES CONGRESS TO THE SECRETARY OF COMMERCE AS EXPRESSED IN TITLE 13, UNITED STATES CODE, CHAPTER V, IS UNCONSTITUTIONAL IN THAT IT LACKS AN INTELLIGIBLE STANDARD TO WHICH ADMINISTRATIVE ACTION MUST CONFORM

That portion of Chapter V, Title 13, United States Code which relates most directly to the defendant is Subchapter II entitled "Population, Housing, Agriculture, Irrigation, Drainage and Unemployment."

The Subsections contained therein read as follows:

"§141. Population, unemployment, and housing

(a) The Secretary shall, in the year 1960 and every ten years thereafter, take a census of population, unemployment, and housing (including utilities and equipment) as of the first day of April, which shall be known as the census date.

(b) The tabulation of total population by States as required for the apportionment of Representatives shall be completed within eight months of the census date and reported by the Secretary to the President of the United States."

"§ 142. Agriculture, irrigation, and drainage

(a) The Secretary shall, beginning in the month of October 1959, and in the same month of every fifth year thereafter, take a census of agriculture, provided that the censuses directed to be taken in October 1959 and each tenth year thereafter, may, when and where deemed advisable by the Secretary, be taken instead in conjunction with the censuses provided in section 141 of this title.

(b) The Secretary shall, in conjunction with the census of agriculture directed to be taken in October 1959 and each tenth year thereafter, take a census of irrigation and drainage."

By virtue of the statutes cited above and similar statutes contained in Title 13, United States Code, Congress has empowered the Secretary of Commerce to obtain information through census and survey. The subsections cited above constitute the full expression of that power as well as the limitations placed upon the Secretary of Commerce acting in his capacity as the United States government's census taker in the areas of Population, Housing, Agriculture, Irrigation, Drainage and Unemployment.

In view of the broad language of Subchapter II, the questions which could conceivably be asked by the census taker would be virtually without limit. As the census law presently exists, it appears that the federal government through the census bureau, could ask its citizens any and all conceivable questions which relate to the broad topics mentioned above. The questions could range from the sublime to the ridiculous, so long as they relate in some way, no matter how remote, to the topics mentioned above. And, if a citizen refuses to answer the questions he does so under threat of fine or imprisonment. The only further limitation to the scope of the questions is contained in the penal statute §221(a), Title 13, U.S.C.A. which provides that the questions must apply to the individual or to the family to which he belongs or is related or to the farm or farms of which he or his family is the occupant. The latter "limitation" accentuates the broad powers of inquiry which the Congress has granted to the Secretary of Commerce as census taker.

At present the census taker can conceivably ask questions of the most intimate nature. Where are we headed? What questions will the federal government ask next? How intimate, how revealing will they be? The answers to such questions should be found in subsections 141 and 142 of Subchapter II of Chapter V above. But those subsections give little or no preview of what is to come, for there is no standard and practically no limit to the inquiry to which the citizens of the United States can be subjected by the census taker.

To allow the census taker to pry at will into the most intimate aspects of individual and family life affords little or none of the privacy guaranteed by the United States Constitution. The Superior Court has reflected on Congress's power of inquiry in the case of Harriman v. Interstate Commerce Commission, 211 U.S. 407, 29 S.Ct. 115, 117, 53 L.Ed. 253, wherein it said:

> "How far Congress could legislate on the subject matter of the questions put to the witnesses was one of the subjects of discussion, but we pass it by. Whether Congress itself has the unlimited power claimed by the Commission, we also leave on one side. It was intimated that there was a limit in Interstate Commerce Commission v. Brimson, 154 U.S. 447, 478, 479, 38 L.Ed. 1047, 1057, 1058, 4 Inters. Com. Rep. 545, 14 Sup.Ct. Rep. 1125. Whether it could delegate the power, if it possesses it, we also leave untouched, beyond remarking that so unqualified a delegation would present the constitutional difficulty in most acute form."

It has long been said that Congress, when delegating power to the executive branch of government must first adopt a policy or set up as "intelligible standard" to which administrative action must conform. Sunshine Cool Co. v. Adkins, 310 U.S. 381, 398 (1940); United States v. Rock Royal Co-Op., 307 U.S. 533, 577 (1939).

In the case of United States v. Rock Royal Co-Op. (supra) the Supreme Court said:

> "In dealing with legislation involving questions of economic adjustment, each enactment must be considered to determine whether it states the purpose which the Congress seeks to accomplish and the standards by which that purpose is to be worked out with sufficient exactness to enable those affected to understand those limits."

Can it be said that the legislative acts which have delegated such broad power of inquiry to the census taker have stated any standards at all? -- The acts speak for themselves.

In Kilbourn v. Thompson, 103 U.S. 168, 195, 26 L.Ed. 377, the Supreme Court cited the failure of an authorizing resolution to state the purpose of a Congressional Committee's inquiry while saying:

> "Was it to be simply a fruitless investigation into the personal affairs of individuals? If so, the House of Representatives had no power or authority in the matter more than any other equal number of gentlemen interested for the government of their country. By 'fruitless' we mean that it could result in no valid legislation on the subject to which the inquiry referred."

In the case at bar the statutes cited above lack a stated purpose which could in some way resemble a "standard to which administrative action (could) conform." And, if such statutes are allowed to remain in effect, the inquiry incident to the exercise of such broad powers can take almost any form and can invade the privacy of individual citizens with the apparent approval of Congress.

ARGUMENT V

THE EXERCISE OF POWER BY THE SECRETARY OF COMMERCE CONSTITUTED AN INVASION OF THE DEFENDANT'S CONSTITUTIONAL RIGHT TO PRIVACY

The Right to Privacy has been defined in Johnson v. Boeing Airplane Co., 262 P. 2d 808 as the right to be let alone, right to be free from unwarranted interference by the public in matters with which the public is not necessarily concerned.

In the case of McGrain v. Dougherty, 273 U.S. 135, 183, 47 S. Ct. 319, 328, 71 L. Ed. 580, the Supreme Court stated two propositions:

> "One that the two houses of Congress, in their separate relations, possess not only such powers as are expressly granted to them by the Constitution, but such auxiliary powers as are necessary and appropriate to make the express powers effective; and, the other, that neither house is invested with 'general' power to inquire into private affairs and compel disclosures, but only with such limited power of inquiry as is shown to exist when the rule of constitutional interpretation just stated is rightly applied."

The aforesaid case shows that while the power of inquiry is an essential and appropriate auxiliary to the legislative function, it must be exerted with due regard for the rights of citizens, and that a citizen may refuse to answer where the bounds of the power are exceeded or where the questions asked are not pertinent to the matter under inquiry.

In Kilbourn v. Thompson, 103 U.S. 168, 190, 26 L. Ed. 377, the Supreme Court said:

> "We are sure that no person can be punished for contumacy as a witness before either house, unless his testimony is required in a matter into which that house has jurisdiction to inquire, and we feel equally sure that neither of these bodies possess the general power of making inquiry into the private affairs of the citizens."

Referring to the authorizing resolution's failure to state the purpose of the inquiry, the court went on to say:

> "Was it to be simply a fruitless investigation into the personal affairs of individuals? If so, the House of Representatives had no power or authority in the matter more than any other equal number of gentlemen interest for the government of their country. By 'fruitless' we mean that it could result in no valid legislation on the subject to which the inquiry referred." Kilbourn v. Thompson, supra, at page 195.

The aforesaid case has been described as one which "will stand for all time as a bulwark against the invasion of the right of the citizen to protection in his private affairs against the unlimited scrutiny of investigation by a congressional committee." In re Pacific Railway Commission (Circuit Court, N. D. Cal.) 32 F. 241 at page 253.

Mr. Justice Harlan delivered the opinion of the Supreme Court in Interstate Commerce Commission v. Brimson, 154, U.S. 447, 14 S. Ct. 1125, 38 L. Ed. 1047 wherein it was said:

> "We do not overlook these constitutional limitations which for the protection of personal rights, must necessarily attend all investigations conducted under the authority of Congress. Neither branch of the legislative department, still less any merely administrative body, established by Congress, possesses, or can be invested with, a general power of making

> inquiry into the private affairs of the citizens. ... We said in Boyd v. United States, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 -- and it cannot be too often repeated -- that the principles that embody the essence of constitutional liberty and security forbid all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of his life."

It has been said that few, if any, of the rights of citizens are of greater importance to their happiness and safety than the right to be free from unauthorized, arbitrary, or unreasonable inquiries and disclosures which delve into personal and private affairs. The Supreme Court has shown in the cases cited above, its recognition of the constitutional limitations on Congressional inquiry.

CONCLUSION

For the foregoing reasons the defendant prays that this Honorable Court dismiss the charge against the defendant.

LAWRENCE M. SULLIVAN
Sullivan, Potter & Roeberg
Attorney for the Defendant
1112 King Street
Wilmington, Delaware

Date: October 7, 1970

MISCELLANEOUS

Before the Federal Communications Commission, Washington, D.C.

[Docket No. 16979]

RESPONSE OF BUSINESS EQUIPMENT MANUFACTURERS ASSOCIATION (BEMA) IN THE MATTER OF REGULATORY AND POLICY PROBLEMS PRESENTED BY THE INTERDEPENDENCE OF COMPUTER AND COMMUNICATION SERVICES AND FACILITIES

Section V.—Security of Data Stored in Computers and Transmitted over Communications Facilities

ITEM J

"What measures are required by the computer industry and common carriers to protect the privacy and proprietary nature of data stored in computers and transmitted over communication facilities, including:

1. Description of those measures which are now being taken and are under consideration; and

2. Recommendations as to legislative or other governmental action that should be taken."

Introduction

In this record-keeping civilization, the person in our society whose name is not inscribed within someone's filing system simply does not exist. Each of us, from birth, begins to deposit information about himself in various public and private files. Our increasing social interdependence assures an acceleration of the rate at which personal data are accumulated and stored.

Moreover, as the Commission recognizes, modern applications in both computer hardware and communication techniques have evidenced a trend toward concentrating commercial and personal data at computer centers. It is thus increasingly possible to collect and retain stores of information concerning various aspects of business and government, and relating to companies, groups of companies, and especially private individuals. The Commission's view is that "[t]his concentration, resulting in the ready availability in one place of detailed personal and business data, raises serious problems of how this information can be kept from unauthorized persons or unauthorized use." (Notice, para. 22). This recognition of the problem has led to the questions raised in this Inquiry concerning measures that are currently available and those that are contemplated to ensure the privacy of personal and proprietary data transmitted over communication facilities.

Certainly the Commission is correct in its recognition of the growth in the automation and centralization of data storage. The utilization of advanced techniques has not only become a necessity if we are to avoid disappearing beneath an avalanche of cumbersome record-keeping techniques, but also provides increased effectiveness in certain vital areas such as medical diagnosis, etc. In brief, personal and business data files, like others, are more and more being transferred from filing cabinets to computers, permitting the collection and storage of more detailed data, its collation in more meaningful form and speedier access to stored data. This practice has been made possible and accelerated by the major advances and innovations made in data processing techniques.

As shown in Attachment 1[1] the growing use of data banks spans a wide scale of government and private industry use. Governmental agencies, both Federal and state, are currently planning and developing major automated data banks. For instance, the Federal Bureau of Investigation is currently piloting the operation of a National Crime Information Center whereby law enforcement agencies throughout the country feed in data concerning stolen automobiles and

[1] Attachment 1, pp. 188–190.

guns, wanted criminals, etc., and receive replies from a central computer complex centered in Washington, D.C. In addition, the Bureau of the Budget is considering the development of a National Data Bank in order to assemble, in a single facility, demographic, economic, and social data generated by present data collection or administrative processes of the Federal government. State agencies are also developing plans for data banks along similar lines, including combination of state tax administration and accounting systems into central files, and instituting data banks in conjuction with the automation of state medical care programs.

Various private industries are also developing data bank systems. Commercial banks, for instance, are inaugurating central information files on their own customers; while credit bureaus are developing central information file systems to assist subscribers in determining credit profiles of prospective borrowers. Moreover, some hospitals are integranting their administrative and medical information processing systems into patient-oriented data banks. Data concerning hospital patients, systematically collected and correlated from medical charts, permits comparative patient studies which can be shared by a number of hospitals.[2]

It is pertinent to note, however, that privacy questions involving stored data are not the result of the development of computer and data processing techniques. The increased concentration of data would have developed in any event, and the computer, while contributing to the immediacy of the privacy problems discussed below, has at the same time, also contributed in major respects to our ability to provide for the secure storage and use of information. As one commentator has stated:

"Centralization of private information and its preservation in computer memories may decrease illegitimate leaks of that information. Those who will have access to personal history will see much more of it than was usually the case when it was contained in printed records, but fewer curious eyes will have knowledge of any part of the private history of the individual."[3]

It can be expected, moreover, that the growing public concern (of which this Inquiry is a part) with regard to the privacy question will itself stimulate greater scientific activity geared to development of systems and devices for the protection of privacy.

Two issues are here involved: (1) Procedures and methods of security control in computer systems and (2) Policy and legal considerations relative to privacy.

1. Procedures and methods of security control in computer systems

The Commission seeks "information on the means now being used or under consideration, and the effectiveness of such measures in insuring that only authorized persons have access to data." (Supplemental Notice, para. 11). In significant respects the degree of security required is affected by the needs of the user in light of the particular data involved; ultimately it will be users who bear the additional costs entailed. In a sense the problem is analogous to the choice that one makes in deciding whether certain records are to be stored in a file cabinet or a burglar-proof safe. Public policy determinations must take these factors into account. At this point, therefore, we append as a matter of convenience an excerpt from Attachment 1, Chapter VI, pp. 192–202, which is directed to this area of Commission interest both in terms of present and future possibilities.

There are effective methods currently available to ensure the privacy and protect the proprietary nature of data stored in automated files

Several techniques currently are available in the use of computer hardware, software, and communications which can be utilized to protect the privacy of data. File protection and other hardware features can be built into the equipment to control access to data. Programmed software can be prepared to ensure the validity of data, and to enforce stringent rules for access to data. Various types of answer back devices can be incorporated into the communication network to identify the source of information requests, and thereby to control dissemination of information.

The effectiveness of programs to ensure the privacy of data is a direct function of the level of effort and expense devoted to systematic planning for utilizing

[2] For a more detailed discussion of the growing use of common data banks, see Attachment I, pp. 188 *et seq.*

[3] Michael, *Speculations on the Relation of the Computer to Privacy*, 33 Geo. Wash. L. Rev. 270, 280 (1964); see also Westin, *Privacy and Freedom* (Atheneum, 1967), pp. 379–380.

the safeguards available in the hardware, software, and communications systems. In general the degree of privacy assured will be dependent upon three factors: (1) physical security of computer equipment and data; (2) equipment and software safeguards; and (3) protection of communications.

Procedures to limit physical access to both equipment and data are employed.—Programs to ensure site security and limited access by unauthorized personnel significantly assist in ensuring the privacy of data maintained in information banks. Such physical procedures include limiting access to:

Actual computer site(s);

Terminals connected to the computer;

Record files; and

Documentation, including operating procedures, systems specifications, and actual software programs.

The principal procedures currently used to limit physical access are discussed below.

Access to the Computer Site or the Terminal is Limited: Access to the computer facility and to terminal equipment is limited to those people actually required to run and maintain the equipment.

Instructions to Operators Are Limited to That Information Necessary to Oper- equipment and do not include any explanation of what the computer is actually ate the Equipment: These consist of specific instructions used in operating the doing, or how to take corrective action in the event of failure of the system. The operators are prohibited access to programs or to copies of file layouts. In addition, all instructions issued by the operator to the computer and all output data received by the operator from the computer are printed by the system and audited by a third party to ensure that proper procedures were followed by the operator.

Diagnostic Software Programs Are Employed to Test the Equipment: Since hardware protective features can be disabled accidentally or intentionally during maintenance checks, diagnostic maintenance programs are employed instead of manual inspection.

Systems Programmers Are Denied Physical Access to Terminals and to Computing Equipment: In general, systems programmers must have full knowledge of the operation of the total system to be effective. This usually includes access to most program documentation and full knowledge of all equipment features. Therefore, it is the practice at many computer installations to deny systems programmers physicial access to the computing equipment.

Both computer hardware and software offer features that can be used to protect privacy—Features available in hardware and software offer protection to systems shared by multiple users and to single users with multiple access stations. These features primarily are designed to protect file records from destruction or alternation, and to limit and control access to data. The significant features are discussed below.

Computer Hardware Controls Access to Data Through Such Features as Memory Read-Write Protection, Bounded Registers, and Privileged Instructions: Many of these hardware features are used in conjunction with software programs to protect data. The memory read-write protection feature prevents unauthorized access to predetermined areas of the computer memory, and may also prevent access to certain computer registers. These features assist in preventing alterations to internal computer instructions, which usually control access to data, as well as protecting file data themselves from destruction.

To illustrate the use of memory read-write protection, assume that a terminal device is limited in authority to access data elements A, B, and C. An authorization table is stored in the computer memory indicating this limitation. If an unauthorized person desires access through the terminal to restricted data element D, he may attempt to alter the authorization table in the memory to indicate that the terminal has authority to access data element D. The memory protect feature would prevent the addition or deletion of any portion of the authorization table stored in the protected area.

Answer Back Features on Communications Terminals Are Used To Limit Access to Data: Many communications terminals contain a feature which permits the computer positively to identify the terminal. When data requests are sent to the computer, the terminal also transmits an identification code which is not under operator control. The computer scans the data request and the terminal identification to determine if this is a terminal authorized to receive the requested data. If the data request is determined to be unauthorized, the computer will

not respond. Unauthorized requests, including the nature of the data requested and the origin of the request, are then recorded automatically by the computer. Authorized personnel in charge of the computer operation may then investigate further the reason for the initial request.

Encryption of Data Transmission Is Used To Ensure Against Interception of Information: Encryption devices are placed both at the computer and at the terminals, and data sent between the computer and the terminals are transmitted in an encrypted format. Data intercepted during transmission therefore are unintelligible to the intercepting party.

Software Is Used As a Major Element for Data Security: Software programs used in conjunction with hardware and communications features provide further protection of the privacy of information. There are numerous software techniques which may be employed. The concepts underlying these are discussed below:

Monitoring: Programmed monitors are developed to detect attempts to penetrate or to record actual penetration of the system. Monitors may provide for recording all rejected attempts to enter the system or specific files, recording the use of illegal procedures to seek access, or recording unusual activities involving certain files or terminals accessing the system. These monitors also can be designed to record or prevent copying of files, as well as attempts to disable hardware or software protection features. Reports of such activities are then produced on a periodic basis, or immediately, for further auditing. If desired, the monitor can be designed to list and analyze all activity within the system.

Passwords: Password codes identifying the user of the terminal may be used. Data requests emanating from the terminal are checked for proper format, terminal identification code, and password code before any response is permitted by the computer. Authorized passwords can be changed frequently to add additional security to the system.

Coding File Data: File data can be maintained in a coded format. This renders a copy of the file unintelligible without the necessary decoding software program.

Wiretapping and induction pose serious threats to privacy of data.—The measures discussed above prevent, or at least detect, invasions of the system. However, wiretapping and induction pose special problems.

Since the cost of physically shielding communications and power cables is prohibitive, there appears to be no practical means available to prevent invasion of the system by wiretapping or induction reception. However, many of the measures discussed earlier tend to reduce vulnerability to wiretapping.

To gain access to specific data, a wiretapper would have to have considerable knowledge of how the system worked. Restricting access to system documentation can assist in withholding this knowledge.

Terminal answer-back features and the use of password identification can obstruct wiretapping.

Coding of file data can hinder simple eavesdropping.

Monitors can assist in detecting the activities of wiretappers.

Scrambling devices can render intercepted data useless to the eavesdropper.

Induction fields, present at terminals, computers and transmission lines, also present security problems. Many advanced terminals use cathode ray tubes for information display and their fields in some cases pose serious shielding and electrical filtering problems. Security requires physically shielding the building or room in which the terminals are housed.

Computers and electro-mechanical terminals also emit electromagetic fields which can be detected from a distance of several miles. [N]oise generation can be used to make [the data used by computers unintelligible to monitors].

4. Future developments will provide increased protection of privacy of computer stored data

One of the major weaknesses in ensuring privacy in an on-line information system is the lack of an automated method of making positive personal identification of persons making inquiries for confidential data. The procedures discussed earlier in this section provide a high degree of security. However, it must be recognized that with sufficient effort it still may be possible for unauthorized persons to gain access to confidential data. For example, it is conceivable that an unauthorized person, despite security measures, many gain access to a computer terminal, have copies of the system documentation, and know the current password employed. Under these circumstances, the unauthorized person would have access to at least some portions of the data held in the computer system, and would appear to the computer as an authorized person with right of access to the data.

37-583 O - 74 - pt. 2 - 62

The development of a method of positive personal identification which the computer could detect would increase significantly the security of data, and a number of automated methods of positive identification currently are being considered. Two such systems now under investigation include the use of voice patterns and fingerprints.

An automated system of voice identification could provide increased security.—Characteristics unique to each individual's voice pattern can be translated into a series of codes. Experiments to date have indicated that the possibility of two individuals having precisely the same vocal patterns is highly remote, and systems that will use voice codes as a method of positive identification are currently being developed. These developments are still in early stages however, and have yet to be proven as a practical and economical system for positive personal identification.

If such a system were successfully developed, voice codes of all authorized personnel could be stored in a computer system. Persons desiring access to data in the computer would speak into a recording device which would translate the voice pattern into a coded form and in turn transmit the coded data into the computer. By matching the input code with the stored code, the computer could provide positive identification of the person involved, and determine which data could be accessed by that person.

Issuers of credit cards have shown interest in the development of an automated fingerprint system for determining positive personal identification.—Under this system, an individual's fingerprint would be coded and recorded in a machine readable form on a card. This card containing the individual's fingerprint would be issued to each person authorized access to computer data. To access the computer system, the card, together with the person's finger would be inserted into a scanning device. The individual's finger would be scanned and a code of the fingerprint developed. A comparison of this code with the code recorded on the card would verify that the card in fact had been issued to the individual seeking access to the computer.

This system potentially could be expanded to transmit such data to the computer, supplying positive personal identification in a manner similar to that used in the voice pattern system discussed above. This system, like voice identification, is still in an early developmental stage.

A positive personal identification system also could assist in detecting abuses by authorized personnel.—A system of positive personal identification for all inquiries to restricted file data could be combined with an auditing system in order to detect abuses by authorized personnel. All requests for information could be recorded by the computer together with positive identification of the requester.

2. Legal and policy considerations

Privacy is an elusive concept which lends itself to a variety of definitions depending upon the particular frame of reference. In essence, however, privacy generally implies the right of an individual (or corporation) to withhold himself and his property from public scrutiny, if he so chooses.[4] More particularly, privacy has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] Since the means for discovering and disclosing information regarding persons and institutions is constantly evolving, the definitional limitations of what constitutes privacy and the situations which conceivably could amount to a recognized invasion thereof, are necessarily subject to corresponding changes.

The scope of privacy is, thus, immensely broad, and voices of concern are increasingly being heard that detail the problems of abuse of privacy on a wide-scale of human activity[6] as well as descriptions of the myriad devices and techniques employed in physical and psychological surveillance of the privacy of individuals.[7] It is to be noted in this connection that centralized stored com-

[4] Black, *Law Dictionary* (4th Ed. 1951).

[5] Westin, *supra*, note 236 at p. 7. Cognizant of the broad scope of the subject, Professor Westin, in analyzing privacy in individual life, recognizes four significant functions which privacy performs: (a) personal autonomy; (b) emotional release; (c) self-evaluation; and (d) protected communication. *Id.* at pp. 32–39.

[6] See, e.g., Westin, *supra;* Packard, *The Naked Society* (McKay Co., 1963); *Brenton, The Privacy Invaders* (Howard McCann, 1964); Ernest & Schwartz, *Privacy—The Right To Be Let Alone* (McMillan, 1962).

[7] *Ibid.* Se also Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's*, 66 Colum. L. Rev. 103, 104–10 (1966); *Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, Right of Privacy Act of 1967, 90th Cong., 1st Sess., pp. 73–86 (1967). The Commission's own recent

puter data is essentially passive, and, in itself, cannot be considered a means of invading privacy.[8] In other words, it is the potential for abuse, once the data is stored and centralized, or in the process of storing and retrieving the data, that gives rise to the problems in this area.[9] The problems that may exist are related to the particular uses to which the equipment is put. Security requirements will vary with the type of use. For example, personal medical information will require greater protection than population statistics available to all from Census sources, which are stored primarily as a matter of convenience.

Although the law erected to protect privacy has traveled an erratic and uncertain path, and has not as yet fully responded to the new situations wherein privacy is a concern,[10] it too must be considered within a particular frame of reference. More frequently than not the question in this regard has simply been whether the law recognized a right of privacy embracing a particular factual pattern. Thus, legal remedies, if any, necessarily vary with the context in which a question of privacy is raised.[11]

From the foregoing discussions and references it can be seen that the general questions of privacy which are being considered both within legislative bodies and by many writers[12] and others in the governmental and non-governmental area, are of major social significance. Even though the perimeters of the area within which the broad privacy question arises and the area within which the Commission may have special or unique regulatory responsibility are not coextensive, the communications portion of the field respecting which the Commission has expressed concern is of significant importance. In considering the role of the Commission in such matters it is necessary, as always, to look first to the Communications Act of 1934. Although the Act itself does not, in so many words, create a general right of privacy.[13] Section 605 does bear directly upon the matter.[14] It provides, in part, that "no person not being authorized by the sender shall intercept any communication [by wire or radio] and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . ." [15] Due, in part, to the sparseness of the record as to any Congressional expression of intent in passing Section 605,[16] its scope and application have been subject to considerable controversy.[17] Nevertheless, it has been judicially stated that the purpose of Section 605 "is to prohibit blatant public or private encroachments on the privacy of messages and the integrity of communication systems." [18]

---

decision in Docket No. 15262 represents an important conceptual recognition of the threat to personal and group privacy through surveillance techniques. *Use of Radio Devices for Eavesdropping*, 6 RR 2d 1691 (1966). Therein the Commission orders a prohibition on the direct or indirect use by private persons of any radio device for eavesdropping on "private conversations" unless all parties to that conversation have consented to the use. *Id.* at 1692.

[8] Indeed, the factor of storage and centralization may itself represent more a method of privacy enhancement than invasion. See Opening Statement, Senator Edward V. Long, on resumption of *Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, Computer Privacy, 90th Cong., 2d Sess., February 6, 1968.

[9] Westin, for example, considers the issue of privacy raised by computerization to be the broad societal one of "whether the increased collection and processing of information for diverse public and privat purposes, if not carefully controlled, could lead to a sweeping power of surveillance by government over individual lives and organizational activity." Westin, *supra*, note 236, at p. 158.

[10] See Lickson, *The Right of Privacy In the Computer Age*, IEEE Computer Group News (January, 1968), p. 13.

[11] Compare, for instance, conditions under which an invasion of privacy would constitute a tort and where, by methods employed, *e.g.* wiretapping, it would amount to a criminal act. Thus, disclosure of confidential information by a credit bureau may represent tortious conduct for which a civil remedy of privacy invasion may be available; whereas "wiretapping" to obtain the same information may subject the wiretapper to criminal liability.

[12] See Harrison, *The Problem of Privacy In the Computer Age: An Annotated Bibliography*, The Rand Corporation, Memorandum RM–5495–PR/RC, December 1967.

[13] *Cf. Daly* v. *Columbia Broadcasting System, Inc.*, 309 F. 2d 83, 85 (7th Cir. 1962) holding that the Communications Act does not create any private rights. See also, *United States* v. *Frank*, 225 F. Supp. 573, 576 (D.C.D.C. 1964).

[14] In *United States* v. *Borgese*, 235 F. Supp. 286 (S.D.N.Y. 1964), the Court while holding that the licensing provisions of the Act and the Commission's Rules do not create a right of privacy, noted that by Section 605, "Congress obviously meant to protect users of telephones against the specified invasion of their privacy as individuals." *Id.* at 291.

[15] 47 U.S.C.A. Sec. 605.

[16] See *Nardone* v. *United States*, 302 U.S. 379, 382 (1937); *United States* v. *Hill*, 149 F. Supp. 83, 85 (S.D.N.Y. 1957). In fact, Section 605 has been described as "a brief, obscure, and undebated clause in that Act—truly a needle in a legislative haystack." Savarese, *Eavesdropping and the Law*, 46 A.B.A.J. 263, 336 (1960).

[17] See, *e.g.*, Article by Francis C. Sullivan, *Wiretapping and Eavesdropping: A Review of the Current Law*, reprinted in *Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, Right of Privacy Act of 1967, 90th Cong., 1st Sess., p. 58, 59–64 (1967); Donnelly, *Comments and Caveats on the Wiretapping Controversy*, 63 Yale L.J. 799 (1954).

[18] *United States* v. *Russo*, 250 F. Supp. 55, 58 (E.D. Pa. 1966).

In other words, notwithstanding questions concerning the scope of Section 605 relating to the type of "interception" [19] and the nature of the divulgence or use, if any, thereafter, it is clear that Section 605 is applicable, in instances where there is initially a communication by wire or radio, to provide substantial protection in the privacy area. That the Commission's concern as a regulatory body is directed to the "privacy of messages [or other data transmitted] and the integrity of communication systems" [20] is reflected in the thrust of the *Notice* and *Supplemental Notice*.

The Commission has stated that Item J "is designed to elicit information on the protection and proprietary nature of data stored in computers *and transmitted over communications facilities.*" (Supplemental Notice, para. 11). (emphasis added.) Further, the Commission has therein specifically disclaimed, as inappropriate, consideration of possible limitations which should be placed on the uses which may be made of the information by those persons who properly have access thereto.

Thus while recognizing as a general social objective—and indeed a crucial one—that it is important for data to be free from unauthorized access ". . . at the computer, the terminal station or the interconnecting communication link" (Notice para. 23) the Commission has emphasized its spcial area of regulatory concern in the integrity of "the interconnecting communication link".

There are many instances of centralized computer storage of data in which there is no "communications" access to the computer from remote locations. The problems of "privacy" may nevertheless be just as important as would be the case if there were also communication of data from a distant location; once the information is in storage the importance of privacy is the same whether the information was stored via communication facilities or otherwise. Nevertheless in these situations not involving the transmission of data communication facilities the Commission would not consider itself to be the expert body for determining the hardware, software, and other techniques to be employed in protecting the privacy of stored data.[21] Neither would it, we believe, consider itself to be a regulatory body which should determine national policy with respect to the privacy aspects of all stored data—whether stored in computer facilities, card files, or otherwise.

Considerations such as those just mentioned reinforce the wisdom of the Commission's delineation, in effect, of its concern in this proceeding in terms of the increasing transmission of data to and from computer facilities via communication facilities authorized or regulated by the Commission and the security of the transmission facilities involved. In the context of possible misuse of these Commission authorized or regulated facilities and the policy questions that may arise, it is worth noting again that in major respects Section 605 [22] would be applicable to protect the integrity of the "communications link" against unauthorized interception and divulgence. Whether the techniques involving communication between remote points and the computer require enlargement of this type of legislative provision to include proscription against unauthorized use of communication facilities to deposit or extract data stored in computer facilities is an area which may well warrant consideration by the Commission. The answer even in this area, however, would seem to depend upon much broader legislative and other policy considerations.

It is pertinent, for example, that in many privacy situations (such as ones involving the area of trade secrets) there are applicable legal doctrines providing a substantial measure of protection to interested parties. Moreover, the unauthorized deposit or extraction of data would seem to present similar basic problems whether or not communication facilities were utilized. Also pertinent here is the highly important fact that the major concerns thus far expressed with respect to privacy problems not covered by Section 605 do not appear to fall within the area of the transmission of data between the remote location and the computer,[23] instead the emphasis is within the area that the Commission has specified to be beyond the scope of the issues in this proceeding, i.e., the un-

[19] For a discussion of the various interpretations of the term "interception," as used in Section 605, see Bradley & Hogan, *Wiretapping: From Nardone to Benanti and Rathbun*, 46 Geo. L.J. 418, 434–441 (1958); see also, *Goldman* v. *United States*, 316 U.S. 129, 134 (1940).

[20] United States v. Russo, *supra* at note 251.

[21] Many of these techniques will, for example, relate to such non-communication matters as site security, personnel selection, training, and responsibility, etc.

[22] 47 U.S.C.A. § 605.

[23] Harrison, *The Problem of Privacy In the Computer Age: An Annotated Bibliography*, *supra* at note 245.

authorized divulgence or other misuse of data by persons or firms properly having possession of the data. (Supplemental Notice, *supra*).

If as a result of available information, including the Responses received in this proceeding, it is the judgment of the Commission that additional regulation or legislation should be considered, we suggest that the most useful approach would be issuance of a more specific statement by the Commission, with a request for further responses from interested parties directed to the particular matters on which guidance is sought.

In summary, therefore, new technology enabling increased data storage is not necessarily on a collision course with the values of personal privacy. This is so because the same technology and expertise that give rise to the problem can, at the same time, be employed to devise systems which will identify and permit beneficial uses of the new technology while precluding those uses considered harmful. Each future use of information storage and transmission may, of course, change the requirements for security. Accordingly, it can be expected that as the requirements become clearer, the ingenuity of the data processing industry and its users will increasingly be challenged to create new mechanisms and methods to guard against the potential for invasion of privacy.

It is important to stress the distinction, in terms of problems of privacy, of a misuse of communications (the indicated area of Commission concern) and a misuse of data of a nature recognized by the Commission to be beyond the scope of this proceeding. The Commission's principal regulatory concern must, we believe, be with the security of the communications link involved in order to assure, to the extent practical, prevention of the unauthorized use of such facilities to invade the privacy of stored data or data being transmitted over such facilities to or from storage. To the extent that broader public policy determinations are required in the exceedingly complex "privacy" area, they would seem to present general legislative considerations involving not only federal, but also state and local interests. Public and private studies are currently underway to develop a more adequate basis for the required judgments. BEMA member companies will continue to cooperate constructively in these important endeavors within their relevant areas.

Respectfully submitted.

BUSINESS EQUIPMENT MANUFACTURERS ASSOCIATION (BEMA),
By JOSEPH M. KITTNER, Esq.,
JOHN S. VOORHEES, Esq.,
Its Attorneys.

ADMINISTRATIVE CONFERENCE OF THE UNITED STATES COMMITTEE ON RULEMAKING AND PUBLIC INFORMATION

RECOMMENDATIONS AND COMMENTARY ON AGENCY COLLECTION AND TRANSFER OF PERSONAL INFORMATION

Definitions

As used in the following Recommendations:

1. "Agency" has the same meaning as that ascribed to it in § 551(1) of the Administrative Procedure Act; 2. "Person" has the same meaning as that ascribed to it in § 551(2) of the Administrative Procedure Act; 3. "Information in Individually-Identifiable Form" means information in such a form that the person who is its subject can be identified by name by any means solely from the information itself; it does not include information in aggregate statistical form. 4. "General request" means a request which is made to ten or more persons, or to all potential recipients of a Government benefit or authorization.

I. COLLECTION FROM DATA-SUBJECT

A. An agency that makes a general request for personal information concerning the respondents themselves should reveal on the form used by the agency to collect the information or on a separate form that can be retained by the respondents: 1. Whether response is a) voluntary, b) specifically required by statute (citing the statute) or c) required by agency regulation (citing the regulation). 2. The use or uses to which the information is intended to be put by the collecting agency. 3. Whether there is any restriction on access to the information in the collecting agency, with a clear and concise statement of the nature of any such restriction, including whether it is imposed by statute (cit-

ing the statute) or by the agency itself (citing the regulation or order). 4. Whether it is specifically contemplated at the time of the request that the information will be provided to particular other agencies or persons in individually-identifiable form, and if so the identity of such other agencies or persons.

B. When an agency makes a request for personal information concerning the respondent that is not a general request, it should provide the respondent with the information described in I(A) if he asks for it.

Commentary

The greatest part of the information collected by federal agencies is obtained directly from the subject of the information himself. At present, agencies generally do not give the respondent any information on whether the information sought is required by law to be furnished, the use or uses to which the information will be put by the collecting agency, or whether the information will be made available in individually-identifiable form to persons or agencies other than the agency which collects the information.

The failure to make such disclosures is not ordinarily attributable to agency ignorance of the relevant information, since agencies are required to supply much of it to the Office of Management and Budget as a condition of securing that agency's approval of any proposed information-collection "from ten or more persons" under the "clearance" procedures established by § 3501 of the Federal Reports Act of 1942, 44 U.S.C.A. § 3501 *et seq.* The non-disclosure policy stems, instead, from a belief by administrators than non-disclosure results in obtaining information people might be unwilling to supply if they knew its intended use, its potential and intended distribution, and the absence of any legal compulsion for them to provide it.

Recommendation I stems from two relatively straightforward premises. The first is that the appropriate basis for government collection of information from its citizens about themselves is a policy designed to achieve their cooperation through informed consent. The second, and related, point is that people often resent supplying information about themselves and their activities without knowing who will have access to the information and the uses to which it will be put.

Fears that the suggested procedure will reduce the volume and accuracy of information provided seem exaggerated in those instances in which the agency can state that provision of the information is required by law (witness the experience of the Census Bureau in taking the decennial census) and in those instances in which, even though not absolutely required, the information is requested in order to enable better assessment of an application for a government benefit or authorization (witness the experience of the Veteran Administration). Even when there does not exist any legal compulsion or any incentive to provide full data in order to obtain a benefit or authorization, programs such as that conducted by the Bureau of Labor Statistics demonstrate the extensive data collection is possible when respondents are given detailed information on how it will be used, and to whom it will be available—at least when restrictions on subsequent dissemination are relatively stringent. In situations not met by the foregoing reassurances, substantial public refusal to provide information on the basis of informed consent must simply be regarded as citizen disapproval of the purpose or the terms of the Government information policy in question. It is the best, and indeed perhaps the only effective, method of registering that disapproval.

It is obviously impracticable to require an agency to attach a description of the data described in Recommendation I(A) to every request for personal information which it makes—for example, a request by the Chairman's secretary for the name, address and business affiliation of a person who is seeking an appointment. Thus, the Recommendation limits the requirement of simultaneous provision of such data to those requests that go to 10 or more persons (the same line drawn by the Federal Reports Act) and those that are standard for all potential recipients of Government benefits or authorizations. Nonetheless, if the addressee of an individual request for information specifically asks to be given information of the type described in Recommendation I(A), it should be provided to him; and Recommendation I(B) so provides.

The term "required" in Subparagraph I(A)(1) is intended to include not merely absolute prescriptions but also a prescription that a person must provide information *if* he is to apply for or to receive a benefit or authorization.

Subparagraphs I(A)(3) and I(A)(4) are not duplicative. There is an important difference between the agency's mere ability to distribute information received, and its actual intention to do so. Subparagraph I(A)(4) is meant to

assure that such an intention will be made known to the person from whom the information is sought. Meaningful compliance will require some agencies to institute recordkeeping procedures that remedy their present low level of awareness of regular information transfers.

The disclosure requirements of Recommendation I apply only when the information is sought from the data-subject himself. Certainly situations can be envisioned in which disclosure would be desirable even with respect to third-person inquiries, but the need is neither as general nor as strong. The natural assumption that response is mandatory does not exist when the inquiry pertains to a third person; and the information sought is ordinarily—almost by definition—not confidential. Moreover, as the Fifth Amendment to the Constitution demonstrates, furnishing information about oneself is considered more deserving of special protection.

II. REGULATION OF INFORMATION TRANSFER

Agencies should take steps to formalize agency policy and procedure on transfers of personal information to other persons and agencies. These should include:

A. The designation of one individual or office within the agency to deal authoritatively with the formulation, dissemination and implementation of agency policy on transfers of information;

B. The compilation and interpretation of all statutes and executive orders applicable to the transfer of information held by the agency;

C. The regularization of frequent transfers of the same types of information to particular other agencies in memoranda of understanding that coordinate agency policies on the collection, storage, and transfer of the information involved;

D. The promulgation of public regulations governing transfers of information in individually-identifiable form which include: 1. Prohibition of transfer of such information, from whatever source collected, to another agency unless (a) Such agency has clear authority to collect the information for the use it intends; and (b) The restrictions on further dissemination of the information are transferred to such agency along with the data. 2. Prohibition of transfer of such information collected from the data-subject to another agency or (where Freedom of Information Act exceptions are available) to any other person unless (a) At the time of collection of the information the provisions of Recommendation I were complied with; or (b) The data-subject has specifically consented to the transfer. 3. Provision for recording in the transferring agency's record of the information the identity of any agency receiving the information, its authority for collecting the data and its intended use. 4. Provision of realistic agency sanctions for violations of the regulations by agency personnel.

Commentary

Few agencies have given systematic thought to the development of consistent policies respecting inter-agency transfer of information. Recommendation II seeks to encourage rationalization and systematic treatment of this sensitive area of activity. Some of the proposals (II(A), II(B) and II(D)(2)) are so clearly desirable even when the transferee is not another agency that they have been extended to that situation as well.

If an agency's decision on the transfer of information is not to be *ad hoc*, it is almost essential that a single person or office within the agency be charged with the formulation and implementation of agency policy on transfers. To our knowledge only the Internal Revenue Service currently has assigned such unified responsibility—to the IRS Information Disclosure Office. The size of the unit necessary to perform such a task will of course vary from agency to agency; in some instances it might consist of a single individual. It would seem advisable, however, to combine authority over inter-agency transfer of information with authority over the processng of requests for information under the Freedom of Information Act. Though the Act does not govern inter-agency transfer, there are obvious advantages to centralizing all information disclosure responsiiblity.

One of the first tasks that should be performed by the agency information office is the compilation in comprehensible and readily accessible form of all statutes, executive orders, existing agency rules and memoranda of understanding governing transfers of information. Expressed awareness of such governing documents is presently very low in agencies generally. Even so information-conscious an agency as the Department of Health, Education and Welfare did not make such a compilation until 1970.

In many cases, however, the statutes governing transfers of information are vague, ambiguous, and even contradictory. For example, in the 150-plus statutes dealing with the subject there seems to be no single meaning of the word "confidential" as applied to data collected by agencies. Sometimes it seems to refer to data that is not to be disclosed beyond the collecting agency for any reason; sometimes to data that is not to be released except for certain vaguely-defined "good" reasons; and sometimes to data that is not to be made public, though it may be shared with other agencies. Thus it seems likely that information offices will have to establish sub-statutory policies and interpretations of statutes governing information disclosure in order to make the statutory compilation useful to agency personnel and intelligible to the public.

A useful technique in rationalizing interagency data transfers is the conclusion of a memorandum of understanding by agencies among whom information is regularly shared. The VA has used this technique to good advantage in exchanges of service record information with the Defense Department and in exchanges of medical information with the Social Security Administration. The agreements specify the statutory framework in which the transfers take place, and coordinate agency policy with respect to the collection, storage, use, and further dissemination of the information transferred. Standard forms are used to obtain the data subjects' consent to the transfers, and to effect the exchanges.

Rationalizing the internal decision-making process will go a long way towards correcting the inadvertent mistakes that occur and eliminating the climate of uncertainty that currently exists in many agencies with respect to the transfer of information. The recommendation that agencies promulgate public regulations dealing with both procedural and substantive aspects of transfer of data in individually-identifiable form is designed primarily to attack another problem: that of public mistrust of agency practices in this area, a mistrust born mainly of ignorance. The fact is that most information exchanges that currently take place are lawful in the sense that they can be reconciled with statutes and executive orders on the subject, and are generally desirable as a means of saving agencies time and money and sparing citizens the burden of multiple demands for the same information. Promulgating public regulations on the subject, then, will have the principal effect of removing needless doubts and suspicions generated by the almost total lack of public information in a field which naturally invites the most imaginative speculation concerning "secret dossiers." Of course the discipline involved in drafting the regulations would also be useful in forcing the agency to make a conscious and intelligent resolution of the many policy problems involved in data transfer decisions—including decisions on when to assert the exceptions from disclosure available (but not mandatory) under the Freedom of Information Act.

The reasons for the recommendations made in II(D)(1) and (2) on the substantive content of the public regulations are largely self-evident. It should be noted that they do not suggest placing any new externally-defined limits on transfers: the agency is left free to determine which transfers to make within limits defined by its own interpretation of the governing laws and its willingness to provide the information specified in Recommendation I at the time of data collection. Where such information has not been given, the "specific consent" requirement of subparagraph II(D)(2)(b) follows the principle established by § 3508(b)(3) of the Federal Reports Act with respect to inter-agency transfers. (OMB has interpreted that consent requirement to apply even when the requesting agency has statutory authority to compel the data subject to supply the information directly.)

The record-keeping requirement of subparagraph (II(D)(3), which is not now general practice, not only is feasible from the standpoint of responsible agency record-management, but also seems essential to the functioning of any monitoring and enforcement system on transfers the agency chooses to adopt. Such record-keeping is of course also necessary to make possible the data subject's right of access to his records proposed in Recomemndation IV. It does not seem feasible to extend this requirement to transfers made to persons other than agencies, and indeed doing so might be thought to contravene the policy of the Freedom of Information Act.

Thought was given to including among the provisions of Recomemndation II an exhortation that agencies use the existing OMB procedures for resolving interagency disputes concerning transfers of information. These procedures are provided for in the Federal Reports Act, which authorizes the Director of OMB to "require a Federal agency to make available to another Federal agency infor-

mation obtained from any person . . .". 44 U.S.C. § 3507. Agencies have usually resolved their differences (in favor of sharing) without outside help, but about a dozen unreconciled disagreements are disposed of by OMB each year. (OMB's record is rather unclear, but it seems generally disposed to disallow transfer where the agency possessing the information objects.) The OMB procedure seems adequate for resolving interagency disputes in the future. Specific mention of it is not made in Recommendation II only because the lack of awareness of its existence which now obtains can be expected to be eliminated when specialized information disclosure offices within each agency are established.

III. GOVERNMENT INFORMATION DIRECTORY

A. Each agency that collects personal information should publish in the Federal Register a clear description of its policy and practice in collecting, using, storing and disclosing such information. The published statement should include: 1. A description of each type of record about persons the agency maintains; 2. A description of the sources from which the information contained in each type of record is collected; 3. A citation to and explanation of the agency's authority for collecting each type of record; 4. A statement of the use or uses to which each type of record is put; 5. A citation to and explanation of the limits on disclosure of each type of record to any other person or agency, including a statement whether the records are released in individually-identifiable form or in the form of statistical summaries; 6. A statement of the conditions under which persons will be given access to all or part of their own records; 7. The name and official address of the agency employee or office charged with the administration of agency information policy.

B. The Office of the Federal Register should periodically compile and publish the agency information-practice descriptions specified in III(A) in a form available to the public at low cost.

Commentary

The pervading characteristic of agency practices with respect to the collection, retention, utilization and disclosure of information is that they are unknown and virtually unknowable. Since agencies have generally not established them with any clarity, attempts by interested persons to discover them often produce nothing except the (erroneous) suspicion that they are intentionally being kept "secret." Thus, one of the purposes of Recommendation III is similar to that of the publication requirements of Recommendation II(D)—the elimination of needless public doubt and suspicion. In addition to this general effect upon the public, Recommendation III will enable particular individuals to discover what information particular Government agencies have about them and from what sources. This may be useful in tracing documents such as birth records; locating information that an individual has already provided when he is asked to provide it again; and identifying situations in which decisions about the individual has been made on the basis of outdated or erroneous third-party information. Publication of agency information descriptions is essential if the right of access to records proposed in Recommendation IV is to have any real value.

Recommendation III will also be of assistance to the agencies themselves, which often do not know and cannot easily discover what sort of information is held by their sister agencies, much less whether or under what circumstances they can obtain it. As a result, it is not uncommon for two or three different agencies to collect, store and use the same sorts of information when a single data base could lawfully and more efficiently meet all their needs. It was to eliminate this sort of waste that OMB's celebrated Kaysen and Dunn reports in the late 1960's recommended establishment of a centralized Federal data bank. The OMB clearance procedure was established by the Federal Reports Act in part as a means of preventing duplication of this sort, but it has been less than completely successful in doing so. Recommendation III will facilitate OMB's efforts and will also enable the agencies themselves to assist in the task.

The proposal of paragraph B that the Office of the Federal Register undertake periodically to compile the agencies' statements assumes that the statements cannot best serve their intended purpose if they are salted throughout the pages of the Federal Register or throughout the various volumes of the Code of Federal Regulations. It is sometimes important for an individual or an agency to know the information practices of a number of different agencies; and the compilation

of such practices in a single volume will facilitate comparison and encourage wider adoption of the best provisions. A compilation similar to the one proposed was attempted in 1966 by the Senate Judiciary Committee's Subcommittee on Administrative Practice and Procedure, published under the foreboding title "Government Dossier." Because the agencies themselves had not, however, undertaken the careful and complete descriptions of their own practices proposed by Recommendation III, that publication is considerably vague and unclear.

IV. RIGHT OF ACCESS

A. Every agency should establish procedures allowing a person to discover on demand: 1. All information the agency holds about the person, except for (*a*) Information specifically required by executive order to be kept secret in the interest of the national defense or foreign policy; (*b*) Information developed in connection with criminal investigations that are still active; and (*c*) Information which would disclose the identity of a regular informant in criminal investigations or an informant who would be exposed to significant risk of physical harm. 2. The sources of the information disclosed (except for informants of the type described in 1(c) above). 3. The identity of other agencies that have received any such information from the agency's records.

B. Every agency should establish procedures allowing persons who are the subject of agency records to submit data contesting the accuracy, completeness, currency and pertinence to the agency's mission of the information concerning them.

Commentary

Recommendation IV is designed to put the Conference on record in favor of agency creation of access rights. To some extent, such rights already exist by virtue of the Freedom of Information Act, 5 U.S.C. § 552, but the present proposal urges the agencies to refrain from applying some of the exceptions available under that Act when a person is seeking information concerning himself. The proposal leaves the agencies free to tailor their access regulations to the particular needs of their own records systems. The minimum requirements, however, should be full disclosure of the contents, sources, and transferees of the information, with the limited exceptions set forth.

An objection sometimes made to relatively unlimited access is that there are some sorts of information, such as doctor's reports, personnel evaluations, and similar information about a person's status or condition that it would be "best" for the person not to know. This paternalistic attitude seems improper for a democratic government, but even if it should prevail the agency can make provision for releasing the information in question to the individual's doctor, lawyer, clergymen, or other personal representative.

A more substantial argument to be made relative to unlimited access is that the best sources of frank and full information about the subject will be compromised (in the most extreme cases exposed to physical danger), potential future sources of information discouraged and pending investigations obstructed. The Recommendation contains exemptions from the access requirements for information as to which these risks are the most substantial and their consequences more severe—notably, information concerning national defense or foreign policy, information developed in active criminal investigations, and information disclosing the identity of regular informants in criminal investigations or other informants who would be threatened with physical harm. For the rest, the Recommendation reflects the judgment that the risk of compromising or discouraging sources of information and of impeding investigations is less to be feared than the opposing risk of causing harm by inaccurate or unfair third party information in agency files.

Concrete experience with access provisions does not support predictions of dire consequences. The most significant experience is that under the Fair Credit Reporting Act, 15 U.S.C. § 1681–84, passed by the Congress in 1970. One of its major features was the creation of the subject's right to demand, for a nominal fee, full information concerning the nature, source and substance of virtually all information contained in files held by credit agencies. Despite doomsday predictions at the time the law was enacted, requests for access have constituted only seven-tenths of one percent of the claims processed by the credit reporting industry since 1970, and there seems to be no evidence of a decline in information on credit reliability because sources have "dried up."

At least one important Federal agency—the Social Security Administration—already provides individuals a right of access to their own records. This has not resulted in a serious drain on funds or personnel, and the agency reports that it has increased both public goodwill and the reliability of recorded data. The *Report of the Secretary's [HEW] Advisory Committee on Automated Personnel Data Systems* recommended that all Federal agencies adopt an access policy based on the principles followed by the SSA.

Paragraph B of Recommendation IV, providing the data subject the right to submit corrections or challenges to his record, is patterned after a similar provision in the Federal Credit Reporting Act. There seems no reason why the successful experience there should not be repeated.

Administrative Conference of the United States

Interagency Transfers of Information in Individually-Identifiable Form

(By Alex W. Bell, Professor of Law, University of Virginia School of Law, Charlottesville, Virginia, September 10, 1973)

This is a report prepared for the Committee on Rulemaking and Public Information of the Administrative Conference of the United States. It represents only the views of the author and has not been adopted or approved by the Conference or any of its Committees.

Recommendations on Interagency Transfers of Information in Individually-Identifiable Form, August 29, 1973

Data Collection

I. In collecting information from individuals, groups or business entities about themselves, agencies should reveal to the respondent at the time of the data collection the identity of the other governmental entities, if any, to which the information sought will be or might be made available in individually-identifiable form. A. The disclosure of the subsequent interagency data activity should be made in writing either on the form used to collect the information sought or on a separate sheet that can be retained by the respondent. B. The representations made to the data subject at the time of collection with respect to subsequent interagency transfer of the information should be recorded along with the data collected.

II. In collecting information about individuals, groups, or business entities from sources other than the data subject, agencies should inform the data subject of the third-party collection activity unless the availability, utility or reliability of the information sought from third-party sources would be thereby impaired. A. In recording information collected from third-party sources agencies should indicate along with the information the date and source of collection and information on the source and the circumstances of its collection that bear on its reliability.

Interagency Transfers of Individually-Identifiable Information

III. Agencies should take steps to assure that they make no transfers of information in individually-identifiable form to other federal agencies that are not clearly authorized by statute or executive order. The steps taken should include: A. The designation of one individual or office within the agency to deal authoritatively with the formulation, dissemination and implementation of agency policy on interagency transfers of information. B. The compilation and interpretation of all statutes applicable to the transfer of information held by the agency to other agencies. C. The promulgation of public regulations governing interagency transfers of information which include:

1. The requirements that no transfer of individually-identifiable information will be made to another agency unless (*a*) The requesting agency clearly has authority to collect the information for the use the requesting agency wishes to make of the data; (*b*) The restrictions on further dissemination of the information are transferred along with the data; and (*c*) The fact of transfer, the identity of the receiving agency, its authority for collection and its intended

use of the information are recorded along with the transferring agency's copy of the data; and

2. Realistic sanctions for employee violations of the regulations.

D. The regularization of numerous transfers or exchanges of the same sorts of information to particular other agencies in memoranda of understanding that coordinate agency policies on transfers of the information involved.

IV. In addition to the steps taken pursuant to III, above, agencies should observe the following guidelines:

A. Agencies should make no interagency transfers of individually-identifiable information obtained from persons, groups or business entities about themselves without the consent of the data subject unless. 1. The data subject has been given notice at the time of collection in accordance with I, above, that such a transfer will or might take place; or 2. The agency is ordered by a court to do so. (a) In the event that compulsory process is sought against the collecting agency to force disclosure of self-supplied information to transferees outside of the scope of the notice given the subject at the time of collection, the collecting agency should notify the data subject in order to secure his consent to the transfer or to allow his participation in the effort to resist the disclosure.

B. Agencies should make no interagency transfers of individually-identifiable information obtained from sources other than the subject of the data without giving notice to the subject of the fact and substance of the transfer, unless 1. The information has been verified by more than one reliable source; or 2. The collecting agency has made reasonable but unsuccessful attempts at verification, yet has reason to believe that the information is probably accurate; or 3. Giving the notice would frustrate a law enforcement or national security interest.

V. Congress should amend the Federal Reports Act, 44 U.S.C. §§ 3501–3511 by adding to § 3508 a subsection (c) which creates a private cause of action cognizable in federal court for "abuse of information," which includes: A. A provision fixing a set amount of damages ($2,000) and the recovery of reasonable attorney's fees to be available directly against any agency making a transfer of informati on in violation of subsections (a) and (b) of § 3508 (or the provisions in III, IV and V, above); and B. A provision extending the availability of the suit to that "information" exempted from coverage in § 3502 of the Act and those agencies exempted from coverage in § 3507 of the Act.

[NOTE: Recommendation V is tentative. Should the Committee approve the principle of private enforcement, I will draft approproate language. It should also be noted that since any private enforcement provision should also be coupled with a legislated access right similar to that discussed in VI, below, it would be perfectly possible to link the two in a more comprehensive legislative amendment to the Freedom of Information Act, which may be a more approproate statute for the Committee to address.]

Right of Access

VI. Agencies should promulgate public regulations specifying the conditions under which individuals, groups and business entities will be given access to their own files. The regulations should include the following principles:

A. Individuals should be given a right on demand to discover at least once every year within a reasonable time after the demand: 1. Whether they are the subject of an active non-investigatory file held by an agency; and, if so, 2. To be told on further demand the substance of any information in their file that has been transferred to other government agencies, the identity of the agencies to which the information has been transferred, and the uses to which it was to have been put by the receiving agencies; Except to the extent that disclosing particular parts of the information in the file would compromise an imminent law enforcement proceeding against the individual, national security, or a pledge of confidentiality made to some third person.

B. Procedures should also be established to allow individuals to correct any factual misstatements contained about them in their records or to contest the accuracy of any information in a short statement to be appended to the data in question.

THE OFFICE OF MANAGEMENT AND BUDGET

VII. The Office of Management and Budget should:

A. Establish procedures to assure that no information collection activity subject to clearance under the Federal Reports Act, 44 U.S.C. §§ 3501–3511 can be

made without a clear and accurate statement on subsequent interagency dissemination of the data in individually-identifiable form as provided for in I, above;

B. Publish periodically, in consultation with other agencies, a clearly-written government information directory available to the public at low cost which includes information on every federal agency with respect to: 1. The sorts of individually-identifiable information the agency records; 2. The statutory authority for the collection and maintenance of the records; 3. The uses to which the information in the records is put; 4. The limits on dissemination of the information in the records in individually-identifiable form; 5. Whether individuals have access to all or part of the information in their records; and 6. The name and address of the agency employee or office charged with the administration of agency information policy.

Almost all federal agencies collect, use and store large amounts of individually-identifiable information about people, groups and business entities as a direct object or a by-product of fulfilling their particular missions. While most of this information-gathering activity tends to be insular, in that the information is not shared with other aegncies, interagency transfers of individually-identifiable information are recurrent ad pervasive enough in the federal establishment to be part of the operational fabric of almost every agency at one time or another, during the course of at least some of its activities.

It seems likely that most of these transfers could be defended as authorized expressly or implicitly by one or more of the 150-plus federal statutes governing interagency transfers of information. It also seems likely that the transfers generally result in time and money savings to agencies and to a reduction of the burden on citizens of responding to multiple demands for the same information.

Nonetheless, it is likely that many of these transfers are unauthorized or outright prohibited by statute and, indeed, that some of them are unconstitutional. Moreover, it is uncontestable that during recent years there has been a substantial outcry against government information policies generally—especially after the proposals for a national computerized data center in the late 60's—cast largely in terms of grim pictures of 1984 and government by secret dossier. While it is difficult to assess the accuracy and typicality of the interagency transfer horror stories that have been bruited in the press and Congressional hearing rooms during recent years, there is no doubt that such stories have eroded public confidence in the information dissemination practices of federal agencies to the point that citizen cooperation with information-gathering by agencies has been impaired.

The purpose of this report is to describe interagency transfer practice and to suggest a set of guidelines to be used by agencies in interagency transfers, guidelines calculated to eliminate popular concern over loss of privacy and to reduce the social alienation which seems to result from some present information collection and transfer practices, without at the same time unduly impairing the legitimate information activities of the federal agencies. These guidelines, then, are an attempted compromise between individual and institutional goals, as any such guidelines must be.

The task of formulating workable guidelines that will strike an apropriate balance between legitimate individual and institutional interests in *every* transfer of *every* sort of individually-identifiable information for *every* purpose between *all* federal agencies is, of course, formidable. The need for agency-specific, mission-specific, use-specific, need-specific, and information-specific data on any discrete proposed interagency transfer of information is essential if the balance of interests is to be struck "right" each time. And in making recommendations of government-wide reach on agency practice, one must also consider the consistency of any proposals with existing applicable statutory law, lest given the choice of massive legislative change or nothing at all, the relevant lawmaking institutions will be insufficiently moved or flexible to respond. Thus in making the recommendations I have sought to propose only what seemed to me the most fundamental requisites for "reform" of current practice, trying to leave untouched for now the haystack of statutes under which transfers are presently made.

Despite the relatively "narrow" focus of this report on transfers of information in individually-identifiable form between federal agencies, it has been a battle—and sometimes a losing one—to confine my recommendations to problems that seemed to be peculiarly associated with data transfers, and not those arising from present agency information policy generally, of which interagency transfer practice is only a part.

Before describing present practices and suggesting changes, I wish to stress that because the scope of the project as defined includes only transfers of information in individually-identifiable form, the recommendations on transfer have little, if any, applicability to data transfers in aggregate statistical form, such as those made by the Census and Bureau of Labor Standards. The use of statistical data is, of course, increasingly important in policymaking and program evaluation, and so long as the individually-identifiable microdata is not implicated directly or indirectly from the size or tabulation method of the sample, privacy interests are not threatened, and interagency transfers of aggregate statistical information are to be encouraged.

I should also note that throughout this report I have used "individual" and personal pronouns such as "himself" to denote both single individuals and organizations of any kind, including business entities.

Finally, it should also be remarked that the guidelines proposed apply equally to both computer-stored and manual access records.

The body of the report is divided into three somewhat overlapping sections. The first deals primarily with the collection of information by agencies and the second deals primarily with transfer of information to other agencies. The format of both of these sections will be a description of present agency practice based on extensive interviews with one or more representatives of 12 different federal agencies, interspersed with recommendations for change. A final section will deal speculatively with the idea of creating a directory of government information activity and an individual right of access to one's own government-held files.

DATA COLLECTION

The vast majority of information collected by federal agencies is obtained directly from the subject of the information himself. In some cases an individual is required by statute to furnish the information sought, as is true, for example, of the decennial census. Even more frequently an individual is required to furnish information about himself as a condition for obtaining a benefit under a federal program, as is true, for example, of the Small Business Administration's loan programs. Finally, some personal information is volunteered solely in the interest of facilitating statistical research, as is the case with respect to the economic reports compiled by the Bureau of Labor Statistics.

One of the most striking findings I made with respect to information-collection from the subject of the data is that agencies do not, as a rule, give the respondent any information at the time of collection on whether the information is required by statute to be furnished, the precise purpose for which the information is being collected, the uses to which it will be put, or whether other governmental organizations will be given access to the information in individually-identifiable form.

The failure of agencies to make such disclosures at the time of collection is not usually a result of inadvertence or oversight, since the Office of Management and Budget's administration of the information-collection clearance procedures of section 5 of the Federal Reports Act of 1942, 44 U.S.C.A. § 3509, requires that agencies seeking OMB clearance for information-collection "from ten or more persons" provide OMB with all of this information as a condition of clearance. The failure to disclose is rather a calculated practice which was uniformly rationalized by the administrators I interviewed—including those at OMB—as a means of obtaining more and fuller responses to demands for information. The theory of keeping respondents in the dark about the authority for collection and the disposition of the information sought is apparently that ignorance of these matters results in a more "cooperative" attitude and honest response.

While there may be some cases in which ignorance results in more reliable and complete information, it seems quite likely that failing to inform respondents of the use and disposition of information sought is one of the major reasons for resentment and suspicion on the part of persons asked to provide information about themselves, and results in a decrease of participation in data-gathering programs and perhaps of the reliability of the information collected. It seems instructive, for example, that the Bureau of Labor Statistics, which depends entirely on a voluntary information-collection, has found it esesntial to give its numerous respondents detailed information on how the information collected will be used and, especially, to assure respondents that the microdata will not be transferred in individually-identifiable form to any other federal agency. Indeed, it is also instructive that almost all the administrators to whom I spoke in preparing this report who defended the practice of information-collection "in the

dark," ironically insisted on full disclosure by me of what I was doing for whom and whether their discussions with me would be attributed to them by name.

Moreover, even if failing to inform respondents of the nature of an agency's authority for collection and of the use and subsequent disposition of the data sought does result in "fuller" disclosure of information, the practice nonetheless seems objectionable because it borders on information-collection by deception or even coercion—either being a low-order governmental interest and a poor public relations tactic, if nothing else. Again, if the growing public outcry over the periodic "exposés" of hitherto "secret" interagency transfers of information is indicative, the pursuance of what-they-don't-know-won't-hurt-them policy towards information-collection, once merely arrogant, is becoming counterproductive as well: there seems to be growing evidence that what-they-don't-know *does* hurt citizens, and agencies pursuing even legitimate information policies, too.

A great deal of the public resentment and suspicion of government data-collection activities could be relatively easily and inexpensively eliminated if agencies simply informed respondents at the time of collecting informaton from them about themselves of the agency's authority and purposes for the data collection and of the uses to which the data will be put. Most importantly for purposes of this report—and a specific recommendation—agencies should always inform the respondent of the identity of other agencies, if any, to which the information sought will be or might be transferred in individually-identifiable form. If the information will be of public record the agency should say so; if it will be made available on demand to law enforcement agencies, the collecting agency should not hide that fact at the time the information is gathered; if it will be guarded from scrutiny by members of the general public, but freely transferred to any other federal agency, the respondent is entitled to know.

The Office of Management and Budget should exercise its undoubted power under the Federal Reports Act, 44 U.S.C.A. §§ 3501–3511, to assure that each agency that must seek its "clearance" before making requests for "information" from "ten or more persons" within the meaning of § 3502 of the Act gives the respondent information on post-collection data activity either printed on the collection form itself or on a separate sheet to be included with the questionnaire, or given and explained to the subject if the collection method is an interview. Agencies or requests for information not subject to OMB clearance should also comply.

This sort of disclosure seems absolutely essential when an individual's or business entity's provision of data about himself is either wholly voluntary or is a condition for the receipt of a government benefit, since it will enable the respondent intelligently to weigh the risk he may be assuming in revealing personal information against the benefit to him of participating in the program of which the data-gathering activity is a part. Some persons might prefer to forego an SBA loan, for example, rather than to provide the agency financial information on themselves that might be later transferred to the FBI under the SBA's policy of full cooperation with law enforcement agencies. In condition-for-benefit cases, of course, the respondent's choice in providing the information may not always be "free," but that appears to be all the more reason to make sure he knows the consequences of his decision. To the extent an agency "loses" important amounts of information or receives an unbearable amount of unfavorable publicity as a consequence of revealing to respondents patterns of interagency data transfer, perhaps the agency's policy with respect to making transfers of that information should be changed. Any transfer legitimate enough to make is likely to be legitimate enough to be accepted by the public.

In cases where an agency is given authority by an act of Congress to compel individuals to furnish certain data about themselves under pain of criminal penalties should they fail to do so, obtaining the individual's "informed consent" to the collection of the information may not be strictly necessary except in cases where the information is being gathered in the course of a criminal prosecution against the respondent. Nevertheless, it seems highly desirable for agencies, even in cases where the respondent must answer, to make full disclosure to the respondent at the time of collection of any certain or likely interagency transfer of the data. Making such a disclosure would probably be only marginally influential on an individual's willingness to provide the information, and could be expected to lessen substantially public resentment of the mandatory reporting requirement. Moreover, it seems possible that disclosing subsequent data activity might actually increase the accuracy of the information collected: disclosure

of the fact that individual income tax returns, for example, are made available to many federal agencies might increase incentive to provide accurate information to both the IRS and the named agencies with whom it shares returns. Even if disclosure of the transfer patterns of information mandatorily supplied results in a public outcry in some instances, the disclosure will have served the useful purpose of triggering a focused debate on a specific agency information activity that might well be needful of change. And such a debate is certain to be conducted in a much better atmosphere than the supercharged climate that has generally characterized the periodic exposés of "secret" transfers of information.

In order to provide accurate information to respondents on data activity after collection, agencies will, of course, have to be aware of with which other agencies they in fact share the information collected. Agency awareness of interagency transfer patterns, I discovered, varies greatly. At one extreme, the Internal Revenue Service keeps rather detailed records on its interagency transfers of income tax returns. In the State Department, however, the expressed awareness of the frequency and number of transfers and even the identity of the other agencies, if any, to whom transfers of passport information were made was quite low. In order to implement the recommendation that agencies disclose to respondents the identity of other agencies to whom information provided will or might be disclosed, then, it may be necessary for some agencies to undertake, at least temporarily, a centralized record-keeping procedure designed to reveal interagency transfer-patterns.

It goes almost without saying that agencies should not make assurances at the time of collecting information that they do not or cannot honor. Lest such a promise be violated out of inadvertence, agencies should record along with any information obtained from a data subject the original agency understanding with the respondent with respect to the use and dissemination of the information outside of the collecting agency. Should the collecting agency for any reason desire to disclose the information to another agency outside the scope of the original understanding with the subject, a specific consent to the transfer contemplated should be obtained from the individual unless circumstances—such as the death of the subject—prevent it.

In addition, agencies should be careful to avoid making pledges of confidentiality they have no statutory authority to honor. A computer-assisted search of the United States Code conducted as a part of the research on this report reveals a conservative figure of 150 statutes that more or less specifically govern transfers of information between federal agencies. A fair number of these statutes arguably require agencies to share information with other agencies on demand. While I discovered no specific examples of unhonorable pledges of confidentiality being made, the 1971 Report of the President's Commission on Federal Statistics cites evidence of such occurences, and the generally low level of awareness of statutory transfer directives I discovered in the agencies I interviewed leads me to believe that there is ample opportunity for such unhonorable pledges of confidentiality to be made.

Thus one of the minimal requirements for any agency desirous of promising an individual that information will be held in confidence is a ready familiarity with the myriad of statutes which, with varying degrees of particularity, govern interagency transfers of information in order to except from such promises transfers to particular agencies with whom collecting agencies must share the information collected. Since many of these statutes are almost meaninglessly broad admonitions to "cooperate" with another agency, collecting agencies may frequently have to resort to formulating intra-agency constructions of the statutes on the question whether transfers will be made under their authority.

Moreover, since at present there is no readily-available source agencies can consult to discover the statutes governing interagency transfers of information, the Office of Management and Budget should undertake in consultation with other agencies a periodic compilation of the statutes governing interagency transfers, perhaps along the lines of the compilation appended to this report. Having one agency authoritatively compile the statutes would be far more efficient than multifarious in-house compilations by each agency, and OMB is the logical agency to undertake the task since it is already intensely involved in virtually all government information-collection programs in the exercise of its clearance powers under sections 3 and 4 of the Federal Reports Act, 44 U.S.C.A. §§ 3503 and 3504. Such a compilation would be valuable not only to collecting agencies in making authoritative assurances to respondents with respect to interagency transfers of information, but also to OMB itself in ful-

filling its duty under the Reports Act to coordinate information collection among the agencies—a duty, I might add, in which it appears that OMB has been very long on talk but very short on action. Such a compilation would also presumably be of interest to a Congress intent on rationalizing the current crazy-quilt of statutes governing interagency transfers of information. The compilation should also be available to the public either separately or as part of an OMB-sponsored guide to government information transactions—a proposal that will be discussed in the concluding section of this report.

Most of the problems associated with the collection of information from primary sources other than the data subject himself involve questions of the propriety of such data collection generally and concerns about the accuracy of the information so collected—problems that are more susceptible of "solution" with resort to the creation of a data-subject's right of access to his files than to safeguards imposed on the collection of the data in the first place. Nonetheless, a few words may be in order about such third-party collection. To the extent secrecy of collection is not absolutely essential to the availability, utility or reliability of the information sought from third-party sources—as may be the case with most law-enforcement activities—the data subject should be informed by the collecting agency that information will be or is being gathered on him, as is the current agency practice with respect to job applicants and candidates for security clearances. Secret data-collection, then, should be avoided unless absolutely necessary.

Collecting agencies should make reasonable attempts to verify the accuracy of any personal information gathered from sources other than the subject of the information himself. More importantly, agencies should be careful in preserving third-party information to record the date and source of the information, the nature of the source's relationship with the subject, and whether the information has been verified from another source. Particular care should be taken in recording unsolicited third-party information to note it as such, because of the high risk of its unreliability. The recording of such data about the source of third-party information is important not only to a proper evaluation of its accuracy by the collecting agency, but also—and perhaps more importantly—to assist a collecting agency in making an intelligent judgment on whether the information is so unreliable that it should not be transferred to another agency at all or, if such a transfer is thought to be necessary, to assure that the information is given no more than proper weight by the receiving agency. To a consideration of current practice and recommendations on interagency transfers of information we now turn.

INTERAGENCY TRANSFERS OF INFORMATION

Before attempting to describe the current patterns of interagency transfers of information, I would like to enter a general caveat and make an observation. First the caveat. No agency that I contacted—or even considered contacting, if the Government Organization Handbook is an accurate guide—had a single individual or office charged with the responsibility of passing on requests for information from other agencies. There is no locus within the government or within a particular agency of information on interagency transfer practices. Since I interviewed only my best guesses of people within each agency conversant with the subject—usually the general counsel's office—I caveat my findings with the admission that I may or may not have seen the agency personnel who could give me the most accurate and complete information on transfer practice and procedure.

Now the observation: while the individuals interviewed were uniformly helpful, I had the sense that by and large they had given very little thought—either formal or informal—to what their agency's present practice and procedure with respect to interagency transfers was, much less to what it ought to be. I also frequently had a sense that I was not asking the "right" questions or was unable adequately to articulate the "problem" I wanted to discuss. As a result I sometimes had the perhaps erroneous impression that interviewees regarded me with suspicion and told me only what I "wanted" to hear.

The patterns of interagency transfers of individually-identifiable information varied widely among the agencies I contacted. At one extreme of the agencies that had definite policies on transfers of information lie the statistical agencies, such as Census and the Bureau of Labor Statistics. These agencies apparently never honor any requests for any individually-identifiable information

from any other agency for any reason. This is so in the case of the Census in part because its organic statute is one of the few statutes that speaks directly and forcefully against transferring individually-identifiable information to other federal agencies. More importantly, both agencies obtain the bulk—and in the case of the BLS, the entirety—of their information directly from the subjects of the information themselves on a strictly voluntary basis, and are therefore dependent on the continuing trust and good will of their numerous respondents for the extensive flow of microdata which form the basis of their statistical reports. Any known breach of confidence would jeopardize or destroy their data-base.

Some agencies that do transfer information to other agencies have regulations governing the practice. While most of these regulations—like those of the FTC—are extremely vague, amounting to little more than an ambivalent recognition of the "common law" practice described below, some—like those of the IRS, VA and SSA—are comprehensive and detailed. The IRS appears to be unique in that it apparently makes some effort to instruct its employees on the guidelines, and even makes an attempt at centralizing the transfer decisionmaking process within the Information Disclosure Office within the agency. Some of these regulations are published, but others—most notably the detailed "operational" regulations of the IRS—are secret. Apparently no agency I contacted, however, has a system of effective sanctions for violations of its interagency transfer rules.

There are some agencies—usually with overlapping missions—that exchange so much information on such a regular basis that they have executed interagency transfer agreements, detailed down to forms: the transfer of service record information between the Defense Department and the VA, for example, is governed by such an agreement, as is the transfer of medical information between the VA and the Social Security Administration. One characteristic of such agreements seems to be that the data subject must give his informed consent to the transfer. Another seems to be that the confidentiality restrictions under which the information is to be held by the receiving agency are specified in detail.

Aside from these and other similar examples, however, the general pattern disclosed by my research appears to be that agencies simply have not given any systematic thought to interagency transfers of information, and as a result requests for information in individually-identifiable form from other agencies are processed on a purely ad hoc and decentralized basis, ungoverned by formal or even informal guidelines more fixed than a case-by-case determination of what is in the information-holding agency's self-interest.

Despite the unregulated and low-visibility quality of much interagency transfer practice, it seems fair to say that there is an overwhelming general bias among agencies—whether or not there are regulations to this effect—towards being "cooperative" with respect to transfers of information to other agencies. No person interviewed suggested that his agency did or should treat requests for individually-identifiable information from other agencies in the same way they do requests for the same information from members of the general public under the Freedom of Information Act. There even seemed to be a casual assumption on the part of some interviewees that the government was more or less monolithic with respect to information obtained from citizens: that if an individual had been willing to give one agency information about himself, there was no reason not to pass that information to another agency—possible differences in the agency missions to the contrary notwithstanding. This general attitude seems supportable incidentally, in light of 44 U.S.C. § 3507, which directs agencies "to cooperate to the fullest practicable extent at all times in making information available to other agencies."

The "common law" of interagency transfers of information that obtains in agencies that have no regulations governing their practice—and indeed, in a fair number of agencies that do—seems to be that if a "responsible" member of one agency makes a request—preferably, but not invariably, in writing—for particular information about an individual or business entity to a person in another agency who has access to the information, and if the party who requests the information states his reasons for needing it—often no more than a bare statement that he wants it for undisclosed "official purposes"—then the transfer of information will be made with no further ado. Generally no inquiry is made into the authority of the requesting agency to gather the information sought, and none is cited beyond perhaps a bare statement of "need." The requesting agency

usually does not inquire and is not told about the confidentiality restrictions, if any, under which the information is held—despite the fact that 44 U.S.C.A. § 3508(a) provides that "all the provisions of law including penalties which relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information."

Nonetheless most transfers of non-public record information are apparently made with the caveat by the agency that collected the information that the information is "confidential"—a term whose precise meaning in the context of interagency transfers of individually identifiable information is cloudy, but appears to be that the information transferred will remain the "property" of the collector, and in any event will not be used by the receiving agency in any way—such as litigation or decisionmaking on a record—that will expose the fact that a transfer has occurred to the light of day—least of all to the individual or business entity who is the subject of the information. Needless to say, no attempt is made by either the transferring or receiving agency to notify the subject of the information that a transfer has taken place, much less to secure the subject's informed consent beforehand.

By far the most striking characteristic of interagency transfer practice is the position agencies generally take toward transferring information collected under an express or implied promise of confidentiality. I gained the distinct impression that a general promise made by a collecting agency to hold certain information "in confidence" is interpreted in many—if not most—agencies as meaning simply that the information will not be disclosed to the general public: a transfer of the information so collected to another agency is not construed to be a breach of confidence. Again, some interviewees seemed genuinely to assume that information collected by one agency "belonged" to the government at large—an attitude belied, of course, by the doubt about the legality of transfers implied by the practice of keeping transfers secret from the subject of the information. While for obvious reasons I was not told directly by interviewers of specific instances in which their agency had breached express pledges of confidentiality made to individuals, almost all interviewers assured me that such practices did occur—at least in other agencies—and the frequent expression of the attitude described above with respect to the meaning of "confidentiality" persuaded me that such transfers are indeed made.

There is substantial evidence that many agencies breach what can be termed "implied" pledges of confidentiality by transferring information to other agencies. That is to say that many agencies—the IRS, FDIC and SBA, for example—know that the individuals and business entities who provide them with information about themselves generally believe that the information will be held "in confidence," even though no express assurances to that effect are generally—if ever—made. Nonetheless, these agencies routinely make interagency transfers of information.

It seems likely that most interagency transfers of individually-identifiable information are perfectly lawful in the sense that they could be rationalized consistently with one or more of the 150-plus federal statutes expressly or impliedly authorizing interagency transfers of information. It also seems likely that interagency transfers of information are generally desirable as a matter of policy to the extent that they result in time and money savings to agencies in collecting information and in a reduction of the burden on citizens ad business entities of responding to multiple demands for the same information. Thus there is nothing "wrong" with interagency transfers of information *per se* unless they are prohibited by statute or constitute an unwarranted violation of the privacy right of individuals to control the dissemination of information about themselves. The apparent furtiveness with which many of the agency personnel to whom I spoke "confessed" to having transferred information to other agencies, then, often seemed puzzling.

The puzzlement disappeared, however, the more I discovered about the unregulated and "confidential" manner in which most transfers seem to be effected. Certainly, if the agencies I interviewed were typical, it appears that the legality and wisdom of most interagency transfer patterns are left to happenstance. As has been noted, I found agency awareness of the myriad statutes bearing on the collection, storage, handling, and dissemination of individually-identifiable information to be quite low. Moreover, most agencies simply had not given serious thought to what their interagency transfer policy should be, or even to what it

was. The circumspection, if not suspicion, born of a vague sense of possible wrongdoing shown by many interviewees was a result.

There are, of course, objectionable aspects of current interagency information transfer practice as (hopefully) any person reading this report can see. Nonetheless these objectionable aspects can in my opinion be largely eliminated without great difficulty or expense, and without at the same time sacrificing legitimate information transfer practices among the agencies.

The first nostrum to be applied is simple: agencies should establish procedures to assure that no transfers of information are made to other agencies that are not clearly authorized by statute or executive order. The legality of interagency transfers, in other words, should not be left to happenstance.

While this proposal is almost truistic, it has within it the seeds of several important reforms. In the first place, it seems essential that agencies designate one individual or office within the agency structure who can deal authoritatively with the formulation, dissemination and implementation of agency policy on interagency transfers, and, to step beyond the scope of this report, information collection and disclosure generally. The transfer officer's duties should include compiling and interpreting statutes governing the dissemination of information collected by the agency, and serving as the point of contact within the agency for requests for information from other agencies or the public.

In interpreting the statutes, agencies should take care properly to interpret provisions mandating simply that information be kept "confidential," since many of not most of them probably interdict transfers of information to other agencies as well as to the public. Transfers should not be made unless "clearly authorized." While the Freedom of Information Act governs interagency transfers only indirectly, in that information that must be made available to the public under the Act can and *a fortiori* should be made available to other agencies, agencies should be guided by the same jealous spirit in which they have apparently interpreted the "privacy" and "business secrets" exceptions to the Act—5 U.S.C. §§ 552(b)(6) and 552(b)(4)—in making disclosures to the public in their transfers of similarly sensitive information to other agencies. While the agency personnel I interviewed were almost uniformly hostile to the idea of formalizing interagency transfer procedures in regulations, I see no other alternative if agency transfer policy is to be rationalized, "taught" to agency employers and implemented consistently within any one agency. The regulations should include a set of intra-agency sanctions for employee violations of the principles and rules set forth in the regulations. It should be the duty of the transfer officer or office to formulate and police the regulations.

An important function of the regulations, and a second reform that might be expected from adopting the recommendation above, is to assure that no transfer can be made without a full awareness of the dissemination restrictions applicable to the information, as well as of the statutory limits on the power of the requesting agency to collect the information sought. There is no reason the regulations could not collate these prerequisites to transfer in some detail by specifying the types of information held by the agency and to which other agencies, if any, that sort of information could be transferred just as IRS regulations do now. The regulatory manual should be public, however, unlike that of the IRS, in order to foster public awareness of agency policy on information activity.

When asked to supply individually-identifiable information of any sort by another agency, federal agencies should always insist that the requesting agency cite its statutory authority for gathering the information sought and specify the use to which the information will be put. Transfers of information should be made only when the requesting agency's authority for gathering the information *for the specified use* is clear. Agencies should be alert in transfer transactions to avoid transfers of information collected for one use to uses that differ substantially from the purpose for which the collecting agency gathered it in the first place, since such transfers may be inconsistent with the statute authorizing the collection.

Agencies should be encouraged to emulate the practice of the VA in regularizing frequent or numerous transfers or exchanges of the same sorts of information to particular other agencies in a memorandum of understanding that coordinates consent, collection, authorization, confidentiality, and use restriction policy with respect to transfers of the information involved. Standard forms are used to effect the exchange. The time and expense savings to be realized from such agreements in ongoing interagency transfer relationships is obvious.

Whenever a transfer of individually-identifiable information is made, the restrictions or lack thereof on dissemination of the information must of course be transferred at the same time. This is probably already effectively required in most transfer transactions by 44 U.S.C.A. § 3508(a), discussed above.

Agencies making transfers should also be certain to record the fact of the transfer, its date, and the name of the receiving agency and the employee requesting the information; the receiving agency's authority for collecting the information; the use to which it will be put, and the portion of the individually-identifiable information transferred. This will be especially important should an access proposal like that discussed in the next section of this report be adopted.

By taking steps to assure that interagency transfers are made only with a full awareness of the legal restrictions already hedging them about, agencies will go a long way towards reforming their current practice. But even legally permissible transfers that are kept secret from the information subject can be criticized on the grounds that they deprive the individual of his statistical integrity if not his prvacy, and that they facilitate secret uses of the information to the subject's detriment. Secret transfers also insulate from public scrutiny an important aspect of agency operations, a situation that leads to suspicion of current practice and creates an impetus for only irresponsible reform. Thus the "hiddenness" as well as the "haphazardness" of interagency transfers should be changed.

Agencies should make no interagency transfers of information obtained from persons, groups or business entities about themselves without the prior knowledge of the data subject that such a transfer will or might take place. As set forth in the first section of this report, agencies should always reveal to the respondent at the time of data collection in clear and specific language the government entities then known to the collecting agency to which the information sought might be or will be transferred. When a collecting agency wishes to transfer information beyond the scope of the notice at the time of collection, specific consent to the further transfer should be obtained. Should the unanticipated transfer be sought in an administrative, adjudicative or judicial process, the collecting agency should notify the individuals or business entities to whom the information sought pertains in order to give the data subjects the right to participate in the effort to resist the disclosure should they so desire. Indeed, while it is related to the scope of this report only tangentially, I would recommend that agencies follow the same procedure in making disclosures to the public of individually-identifiable information under the Freedom of Information Act. Thus unless an individual were notified at the time of data collection that the personal information be supplied would be available to the public, the agency should obtain the consent of the data subject prior to its release or notify him of any effort to compel its disclosure.

It seems self-evident that agencies should honor their understandings with data subjects about the scope of permissible dissemination to other agencies of information they provide about themselves. Transferring information collected under an express or even implied promise of "confidentiality" constitutes deception of the worst sort. There can be no doubt that such practices—when they are revealed and even when they are suspected—increase alienation on the part of citizens and undermine their confidence in the integrity of the government generally. It seems imperative, then, that agencies guard information obtained under a blanket promise of "confidentiality" from disclosure to other agencies as well as the general public. Indeed, it is arguable that almost all agencies are usually required to do so by 44 U.S.C.A. § 3508(b)—a portion of the Federal Reports Act—which provides that no information obtained by any federal agency by a means that requires clearance by OMB may be transferred to another agency unless (1) it is in the form of statistical summaries; or (2) it was not collected under a pledge of confidentiality; or (3) the individual supplying the information gives his consent to the transfer; or (4) the agency to which the transfer is to be made "has authority to collect the information itself and the authority is supported by legal provisions for criminal penalties against persons failing to supply the information."

Of course, honoring understandings with the data subject at the time of information collection as to the subsequent dissemination of the information may have the effect of at least temporarily inhibiting the interagency transfer of some information that is presently exchanged. Any transfers that will be inhibited, however, are almost certain to be those most suspect under present practice. It is important to note, moreover, that the recommendation that agencies follow what I have called the informed consent model in the collection and

dissemination of information need not and should not be taken as a call for agencies to engage in totally insular and redundant information-gathering exercises. It imposes no independent substantive limit on information transfers that is not within the exclusive control of the collecting agency itself through the assurances it makes when it collects information: lawful transfers can be made so long as notice is given the subject either at the time of collection or consent is obtained at the time of transfer.

The proposal does of course make it important that agencies be thoroughly familiar with the stautory limits on transfers of the information they collect and, as importantly, that they carefully weigh the importance of their current interagency transfer relationships against the costs in losses of good will and perhaps even information that might result from revealing those relationships to the information-supplying public. These consequences do not seem undesirable. In any event, however, one can be confident that any losses of self-supplied information currently being transferred without the knowledge or consent of the data subject will in the long run be more than outweighed by the gains in public confidence—and perhaps information—that following the consent model would produce. And any inefficiencies that might result from following the model could be expected to be offset by interagency memoranda of understanding like that discussed above, and by the publication and use of a government data directory of the sort discussed in the final section of this report.

While the matter is not entirely free from doubt, in my judgment one agency should be able without the knowledge of the individual involved to reveal on demand to another agency authorized to obtain the information whether or not it maintains a record of self-supplied individually-identifiable information on a particular person, group or business entity, as is now the practice of the IRS in response to requests for "tax checks" routinely run, for example, on potential executive appointees. Virtually all agencies contacted respond to similar "agency check" requests on government job applicants from the Civil Service Commission, though it appears that the applicant is informed that such a government-wide check for records on him will be run. While there can be no doubt that information on the mere existence or not of particular sorts of records may be at times *prima facie* damaging to an individual—such as whether he had filed an income tax return or whether he had a conviction record on file with the FBI—my impression is that the number of cases in which agency knowledge of the mere existence of a record gained without the consent of the data subject is actually used to the detriment of the individual without providing him with an opportunity to explain away any potential embarrassment are quite limited, and in any event are not substantial enough invasions of privacy interests to warrant preclusion across the board so long as the consent model is followed in the transfer of the actual data in the record.

Self-supplied information obtained under a statutory mandatory reporting requirement or court order should not be transferred to any agency beyond the scope provided for in the statute or coercive order unless consent to the specific transfer is first obtained from the subject of the data. This requirement is not only desirable from the standpoint of reducing public resentment of coerced collection in any case, but may also be constitutionally compelled by the 5th Amendment when the requesting agency is seeking the information in order to facilitate criminal prosecution of the indivdiual data subject involved.

One is tempted to conclude *a priori* that transfers of information obtained from sources other than the subject of the data should never be made without first informing the subject of the content and obtaining his consent to the transfer. This is so not because the information is necessarily less reliable than self-supplied data—although safeguards on reliability seem especially appropriate here—but because of the possibility of the *use* of such data to make a decision affecting the status of any individual in a way he would consider detrimental without at any time in the course of the agency action informing the party affected of the existence of the information or giving him a chance to challenge its reliability. The risk of secret detrimental *use* of data, however, is not confined to third-party information or even "transferred" information and presents a due process problem that in my judgment goes considerably beyond the exigencies presented by the limited subject in this report. Moreover, it seems quite likely that as a general proposition the institutional interests in transferring third-party information outweigh the individual interests in controlling the transfer of such information simply because it is by definition more "public" than self-supplied data and the individual's claim to control over the transfer

is not particularly strong. This is especially so if it is law enforcement agencies that carry on the major trade in such data, as one would expect, since their "trade" tends to be incestuous; in any event the due process safeguards on the use of any information for law enforcement purposes is the most "adequate" we have. The safeguards on transfers of third-party information set out in the next paragraph seem adequate, especially if individuals are given a right of access to information about them in agency files, as discussed in the next section of this report.

Interagency transfers of information obtained from sources other than the subject of the data should not as a rule be made without giving notice to the subject unless the information has been verified by more than one reliable source—or preferably, checked for accuracy by the subject of the information himself under an access proposal like that discussed in the next section of this report—and unless it is clear that the requesting agency has authority to gather the data and the notice to the date subject would not frustrate a law enforcement or national security interest. Unverified information can be transferred between agencies that share the responsibility for instituting or prosecuting civil or criminal actions against the same individual when the information is germane to the performance of the agencies' joint mission. Transfers of this sort routinely take place between the FTC and the Antitrust Division of Justice, for example, and seem to be necessary in order to coordinate enforcement of the antitrust laws. Any agency can release unverified third-party data to another agency without gaving prior notice to the subject if the collecting agency has made reasonable, but unsuccessful attempts at verification, believes from the nature of the source's relationship with the subject or other circumstances surrounding the collection of the data that the information is probably accurate and is persuaded that the requesting agency has authority for the collection and the use to which the information will be put is not significantly different from the use for which the data was collected. The more sensitive the unverified data, of course, the more certain the agency should be of its accuracy before revealing the information. Whenever a transfer of third-party information takes place, the third-party nature of the information and the status of its verification should be transferred at the same time.

Unsolicited, unverified third-party information should generally not be transferred at all except between two or more law enforcement agencies in the course of an active criminal investigation or prosecution. The nature of the information should of course be noted in the same transaction.

Devising a system to assure compliance with the guidelines on transfer in addition to the intra-agency "realistic sanctions" recommended above presents a difficult problem in a choice of enforcement techniques.

As has been ably explored in Arthur Miller's *Assault on Privacy*, 173–209, at present individuals aggrieved by interagency transfers of information concerning them have no effective private remedy against offending agencies, even if they could discover a transgression in the first place. The common law theories of libel and privacy are not easily tailored to redress many of the sorts of injury suffered by an individual in a transfer situation, the costs of litigation compared to the predictably small amount of recovery arel ikely to discourage all but suits brought "on principle," and the doctrines of sovereign and official immunity could be expected to take their usual toll on the few cases that might overcome the first two hurdles. While the celebrated *Bivens* case raises a remote possibility that there could be a federal constitutional tort of invasion of the "1st-4th-5th-9th amendment penumbral" right of privacy, there is no reason to believe that its scope of coverage would be any broader than its common law analogue—although it could not, presumably, be barred by sovereign or official immunity. There are at present no statutes expressly authorizing an individual to sue officials for disclosures made in violation of federal law.

Nor does there appear to be any obviously effective public law remedy for unauthorized transfers, though this is not because there are no statutes creating them on the books. Indeed, a search of federal statutes on information transfer revealed a plethora of criminal statutes dealing with disclosure of information, the most general provision being 18 U.S.C. § 1905, which establishes the penalty of removal from office or employment as well as a fine of up to $1,000, and imprisonment of not more than one year for any federal officer or employee who:

> publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment . . . which . . . concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confi-

dential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation or association. . . . The statute's major use, however, has been defensive, as an unsuccessful means of resisting disclosure of information under the specific statutory exemption portion of the Freedom of Information Act. See, e.g., M. A. Schapiro & Co. v. SEC, 339 F. Supp. 467 (D.D.C. 1972). Indeed, there are no reported instances of its enforcement, and none of the agency personnel I interviewed could recall enforcement of § 1905 or any other criminal prohibition on disclosure. This might be explained, of course, by impeccable administrative behavior. A more likely explanation, however, is a combination of the inherently undetectable nature of the "crimes," the uncertainty whether many of the statutes actually outlaw disclosures of information to other agencies as opposed to the public at large, the "insider" perspective that would be brought to bear on a decision whether to prosecute, and perhaps even the seeming severity of the penalties involved. The only other generally applicable statute restricting the dissemination of "confidential" information, incidentally, is that portion of the Federal Reports Act discussed above, 44 U.S.C. § 3508(b), and it is purely hortatory, supported by no sanctions at all.

It is certainly possible, of course, that an individual or class of individuals "aggrieved" by one agency's action in transferring information to another might be able to persuade a court to enjoin the practice if it were persistent enough, to mandate its expunger from the records of the receiving agency, to reverse a decision based on an improper use of the information, or perhaps even to grant damages, at least in cases where the transfer or its use was unconstitutional, in clear violation of a statute or constituted an abuse of discretion. The difficulty with remedies available on judicial review under the APA, however, is in part the same as with all the present private common law remedies for unauthorized transfers—namely the difficulty of detecting abuses in the first place, the prohibitive expense of bringing a suit once the abuse is discovered, and the likelihood that an award of damages, if made, would be extremely small.

A simple and in my judgment effective method of creating agency incentive to comply with the statutes governing interagency transfers and the recommendations in this report would be to create a statutory private cause of action for "abuse of information" which would include a provision fixing a legislated amount of "actual" damages and the recovery of attorneys' fees to be available directly against any agency making an unlawful transfer of information. The provision of such a cause of action would almost have to be accomplished by a legislated "right of access" provision like that discussed in the next section. The simplest method of creating the "abuse of information" tort would be to add a section (c) to 44 U.S.C. § 3508 which provides simply that violations of the provisions of subsections (a) and (b) could be redressed in a suit in equity or action at law against the agency making the transfer cognizable in federal courts, and providing for the recovery of reasonable attorneys' fees and a minimum amount of damages—say $2,000—recoverable over against the offending employee by the agency. A special provision would have to be added dealing with the few agencies and sorts of information-gathering clearance procedures—most notably the IRS and inquiries made of federal employees.

The private cause of action, coupled with the agency sanctions that would be created under the regulatory recommendation made above, would, it seems to me, maximize agency and employee incentive to comply with the safeguards.

My recommendation on this point, however, is tentative in that it may be that making the safeguards enforceable (assuming Congress could or would act quickly on the "abuse of information" and "right of access" measures) at the same time the safeguards are established may make agencies leery of adopting the safeguards at all—a measure that under the recommendations does not turn on legislative reform, but is left solely to agency initiative. Or even if agencies adopted the safeguards suggested above on paper, too effective a sanction might simply drive transfers "underground." It may well be that agencies would be more comfortable—and likely to act—with establishing only their own agency sanctions before private parties are allowed to enter the picture. Indeed, it is possible that even the APA review proceeding might become effective enough to deter serious abuses if access to one's records is provided.

A RIGHT OF ACCESS AND A DATA DIRECTORY

At several junctures throughout the preceding sections of this report I have alluded to the desirability of creating an individual right of access to records

about oneself as a means of assuring the accuracy of information collected from third-party sources about the subject of the information, as a means of providing individuals with a method of determining whether their records were being abused for purposes of suit and, indirectly, as a means of increasing public confidence in the data collection and transfer practices of the government generally by making them more open.

While one might readily agree that an access right in the abstract might be *a priori* desirable for most agencies to adopt, one might justifiably wonder if such a recommendation is warranted solely as a corrective for interagency transfer problems. Moreover, the difficulties of structuring specific government-wide guidelines on an access right are formidable. The costs of providing access, for example, might be prohibitive for either the individual or the agency in some cases where the individual's "record" may be dispersed in a half-dozen different offices of an agency, or stored in such a manner as to be virtually irretrievable. More than one interviewee assured me only half-jokingly that the major "problem" with his agency's present information policy was that once a "bit" of information was put in his agency's files, finding it again was a virtual impossibility. Along the same lines, establishing the geographical location in which a person's record might be made available to him could present difficult problems for an agency that could not or should not be resolved by the use of a device such as providing access through the mail. The frequency of access presents similar difficulties. Finally, while I am not generally sympathetic to withholding from the individual about whom the information pertains information such as doctor's reports or personnel evaluations, it is obvious that there are some sorts of files—especially investigatory files compiled for law enforcement purposes and files required to be kept secret in the interest of national security—that should not be available to the individual about whom the information pertains least the achievement of extremely important social values be compromised or frustrated as a result.

Lest any such recommendation seem radical to some administrators genuinely concerned about the impact of a right of access on the performance of their missions, however, it should be pointed out that the principle of access to one's own records is already embodied in the Freedom of Information Act, and agencies can draw on their experience under the Act to gauge and deal with most of the problems likely to be encountered under an access scheme. It should also be pointed out that at least one agency—the Social Security Administration—already allows individuals a right of access to their own records seemingly without serious drains on the time, funds or energy of the agency, and indeed, apparently with some gains in goodwill and the reliability of the information it holds. Moreover, the HEW *Report on the Secretary's Advisory Committee on Automated Personal Data Systems* in late July of this year recommended that all agencies adopt an access policy far more extensive than the one suggested below.

Congress created a model for a legislated access right when, in 1970, it promulgated the Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681–1684t which, among other provisions requires in § 1681g(a) that an individual has a right upon demand and for a nominal fee to be fully informed of the nature, source and substance of all information contained in his credit file except for medical information and the sources of information contained in an undefined "investigative" report. Individuals must also be notified by the user of the name and address of the credit reporting agency who supplied the report any time the user takes adverse action against an individual such as the denial of credit or employment, based in whole or in part on such a report. Despite dire predictions by credit agencies that their sources of information would dry up and they would be deluged by requests for access to reports by disgruntled or merely curious individuals, Professors Westin and Baker in *Databanks in a Free Society* report that after a "flood" of requests during the first 10 months in which the Act was in effect, requests in one representative credit reporting agency dropped off dramatically and levelled off at seven-tenths of one percent of the total inquiries processed—a rise of only two-tenths of one percent in such requests from the time prior to the effective date of the Act (p. 138). And I am aware of no data suggesting that since April 1971 banks and retail marketing institutions have been unable to obtain information on a debtor's credit reliability because credit reporting agencies sources have "dried up."

The Fair Credit Reporting Act experience has not gone lost on Congress, and almost word-for-word applications of the Act to federal agencies have been entertained with what seems to be growing support in the last few sessions of

Congress—for example, H.R. 9527 and H.R. 15613, both by Representative Koch of New York, during the 1st and 2d Sessions of the 92d Congress, respectively, and both of which would have created a new Freedom of Information Act section that provided not only for access at cost, but also that agencies must notify every person on whom the agency maintained a record that the agency did so, and notify the person each time the agency augmented his record with third-party information. Hearings were held on 15613 before Representative Moorehead's House Government Operations Subcommittee in May of 1972.

Pending legislative amendment of the Freedom of Information Act along the lines of the Fair Credit Reporting Act—a move that seems bound to come—and ignoring for the moment details of time, manner and place that could be expected to be best resolved on an agency-specific basis, it seems desirable for the Conference to go on record in favor of at least a rudimentary form of access to one's own records that could be implemented by agencies with no change in statutory law.

Agencies should undertake steps to promulgate public regulations specifying the conditions under which individuals would be given access to their own files. The regulations should include at least the following principles:

Individuals should be given a right on demand to discover at least once every year within a reasonable time after the demand whether they are the subject of an active non-investigatory file held by an agency and, if so, to be told on further demand the contents of their file, the identity of any other governmental organizations to which the information has been transferred, and the uses to which it was to have been put by the receiving agency, except to the extent that disclosing particular parts of the information in the file would compromise an imminent law enforcement proceeding against the individual, national security, or a pledge of confidentiality made to some third person.

Procedures should also be established to allow individuals to correct any factual misstatements contained about them in their records or to contest the accuracy of any information in a short statement to be appended to the data in question.

One of the main particulars in which the proposed recommendation on access differs from that embodied in the Koch "Citizen's Privacy" bills mentioned above is that the access would be triggered only on the demand of the individual who wishes to see his records. In order to facilitate intelligent demands for access and as a result, incidentally, to reduce the net number of demands made on agencies as a whole, agencies should publish periodically a catalogue of authority for their maintenance, the uses to which the information in the records is put, the limits on dissemination of the files to private and governmental organizations beyond the collecting agency, whether individuals have access to all or part of the information in their records, the name and address of the agency employee or office charge with the administration of agency information policy, and similar information that would be useful to an individual (or agency) desirous of informing himself on the information policy followed by a particular government agency. Professors Westin and Baker, in *Databanks in a Free Society*, have felicitously styled a proposed low-cost compendium of such agency catalogues a "Citizen's Guide to Files." "The emphasis in such a booklet," they state, would be on clearly written, detailed descriptions so that sensitive files of information would not be masked by the general nature of a description or lost in a trailing "et cetera."

> The great value of . . . [the proposed guide] is that it would provide the citizen with a thorough, detailed, and nontechnical directory of the record systems that contain information about him, and the general rules under which it is being held and used. (p. 363)

Another benefit to be realized, of course, is the facilitation of interagency transfers of information within the statutory limits imposed on such transfers—transfers that could save time and money for both citizens and agencies, but which may be forgone at present simply because of agency ignorance of shared information needs borne of the sheer size and complexity of the federal information apparatus.

While Westin and Baker suggest that the initial preparation and periodic updatings of such a guide be undertaken by a legislative committee such as the Government Operations Committees of Congress, it is my judgment, as has been indicated at various points above, that the Office of Management and Budget, being charged as it is with the administration of the only general federal information collection and transfer statute—the Federal Reports Act—

is far better fit to perform the task of compiling such a guide both from the standpoint of its already-existing expertise in the area and from the respect (or even fear) it seems to command from other federal agencies. OMB already collects a great deal of the information from all federal agencies that would be needed in order to compile such a guide, and in any event has available to it the use of the pervasive clearance power apparatus to secure any detailed information on most agency collection and dissemination transactions that might be necessary to make the guide authoritative, up-to-date and complete. The guide should also be of enormous help to OMB itself in its administration of the Reports Act mandate to coordinate collection efforts among the agencies.

While in this report the data directory proposal is linked to the proposal for the creation of a right of access, I wish to make clear that the recommendation on the data guide is severable, and should be adopted even if the Conference should wish to take no position on the access proposal at this time.

CONCLUSION

While at present interagency transfers of information in individually-identifiable form are effected by and large in an *ad hoc* and decentralized manner, the mere fact that this area is unregulated does not mean that all *ad hoc* interagency transfers are unlawful or necessarily undesirable. It does, however, mean that the legality and desirability of making particular transfers is left largely to happenstance. It also means that the transfer decision-making process is probably inconsistent within various field offices of the same agency because it is uncoordinated. And finally, it means that most agencies' transfer practices remain unknown and undiscoverable—and as a result suspect—by individuals asked or required to provide agencies with information about themselves or others, and by other agencies who might be desirous of making a perfectly lawful and economical additional use of data already held by an unknown second agency. Thus there are "problems" with present interagency transfer practice that can and should be solved. The recommendations in this report are designed to do that in a way that will involve a minimal incursion on legitimate agency information practices and no changes in existing laws. That is not to say that a rationalization of the present welter of statutes wouldn't be desirable or that future recommendations of changes in agency practice might not be appropriate in the future.

And to echo a theme sounded first at the beginning of this report, it seems important to remember that interagency transfers of information are only a small, perhaps even parochial, part of the universe of important issues that are raised by current governmental information practices—the propriety of collecting or recording some sorts of information at all, the propriety of the use of some information or even blacklists by agencies to make judgments that affect the lives of individuals significantly without giving the person affected notice of the basis of the decision, and the problems associated with the "dating" of information with an eye to removing it from records altogether at the end of its useful "life," to name a few. Thus there are many changes in current agency information practice that may be desirable or even necessary that are not touched on in this report simply because they are not warranted as a response to the narrow range of information practices I was charged with studying.

Nonetheless interagency transfers of information are an important part of current agency practice and their regularization along the lines suggested in this report should result in benefits in the form of public confidence in the integrity of government information activity. Agency response to these recommendations will form an appropriate point of departure for self-initiated efforts at a more general reform, perhaps along the comprehensive lines of that suggested in *Records, Computers and the Rights of Citizens* (the HEW Report of the Secretary's Advisory Committee on Automated Personal Data Systems), or the National Academy of Sciences-sponsored tome by Professors Westin and Baker on *Data-banks in a Free Society*. It is obvious, for example, that when agencies give notice at the time of data collection of the other agencies to whom the information will be available they may well want to give full notice at the same time of the nature of the agency's authority for collection, as well as details on its intended use. These recommendations, then, should be regarded as only a beginning of the process of achieving that openness that should be the mark of individual record-keeping by agencies in a government that belongs to its citizens.

Report on LITE Computer Search of U.S.C. Provisions on Interagency Transfers of Information, August 9, 1973

(Prepared by Mr. Frank Thomas and Mr. Carl S. Mallow, Chief of User Services Section, Air Force LITE Computer System, under the direction of Professor Alex W. Bell, University of Virginia Law School)

The statutes compiled in the following lists deal only with transfers and use of information knowingly furnished by individual entities outside of the government to entities within the government; no attempt was made to uncover statutes that deal with transfer of data that has been generated by the government itself, such as results of criminal or civil investigations or of government-sponsored experiments and research. While the scope of the search appears to have been fairly exhaustive, especially in the case of statutes restricting the use of information, there are undoubtedly more statutes on the subject than are sumarized in this report.

The search was performed by the Air Force's LITE computer using tapes of the entire United States Code on the basis of linguistic scanning instructions—such as "print out summaries of all statutes in which the phrase 'confidential information' appears," or "print out summaries of all statutes in which the words 'information,' 'disclosure,' and 'except' appear separated by no more than 10 other words." With the able assistance of Mr. Carl Mallow at the LITE center in Denver we cast over 100 "word nets" in 14 basic runs on the computer, trying each time to pare down the number of statutory "fish" we caught to only those directly relevant to this project.

Because of inevitable "holes" in our "nets," the searches may well have missed many statutes that govern interagency transfers of information. Moreover the search may have missed some statutes that are in fact used by agencies to control information transfers because of the attitude sometimes taken by agencies that information transfer policy may be governed by general statutes which on their face give only slight indication that they might be relevant to information transfer. A final gap in the coverage of this survey may be indicated by the fact that some statutes seemingly "assume' that restrictions on the dissemination of information generated under the statute will or should be imposed in situations in which the agency, the person furnishing the information, or "reasonable men" would consider the information to be confidential, without explicitly mandating the establishment of a procedure for such an ad hoc "classification" of the information generated under the statute.

Because of these gaps the statutes presented should be deemed to be more an exhaustive survey of the various techniques used to control the process of information transfer among agencies than to be a complete listing of all United States statutes governing interagency information transfers.

An attempt was made to place statutes and in many cases subsections of statutes into more or less archtypical categories in an effort to distill patterns of statutory regulation of interagency transfers of information. There are, as a result multiple listing of some of the statutes.

The "patterns" of regulation into which the statutes are now grouped are somewhat overlapping and may be for the most part either too amorphous or too ambiguous to be of much value. Nonetheless, one interesting, if not surprising, "pattern" emerged so strongly that it deserves mention at this point: the statutory restrictions on interagency transfers of information appear to be a crazy-quilt. While one might have thought that the computer searches would reveal a rational Congressional "policy" towards at least what sorts of information must *always* be exchanged and what sorts of information must *never* be exchanged, the statutory provisions indicate that there simply is no such consistent policy. Even information of the same "degree" of sensitivity—in that all reasonable men would agree that information of that sort should not be disseminated at all (or, perhaps, even collected in the first place) because of its high potential for harm or embarrassement to the individual or entity to whom it relates—is sometimes explicitly protected from disclosure to any person or agency, at other times is explicitly made "public," and at yet other times is left to the unfettered discretion of an agency whether to make it public or not without any discernible differences in the nature of the "public interest" that might require the different treatment. A highly significant fact is the failure of the search to turn up any consistent general definition of the term "confidenial," which seems to be the key word in most schemes of restriction on information dissemination.

The statutory regulation of information transfers, in other words, appears to be an extremely hodgepodge effort, with no real consistency as to subject matter or technique. This general lack of rationality makes one suspect that the subject of information transfer is often tacked on to a statute as an afterthought rather than as part of a comprehensive regulatory scheme, and that the subject is therefore ripe for legislative reform.

I. STATUTES AUTHORIZING TRANEFERS OF INFORMATION

I A(1)

These statutes are a small sampling of the many that deal with the transfer of information between agencies only in that they appear to require or empower agencies to co-operate with other agencies. Assuming the power to transfer information to other agencies does not have to be specifically delegated by the legislature, statutes like these could be said to "authorize" interagency transfers of information. These provisions in fact seem to be "throw-aways," put in statutes to make sure that there is no unnecessary duplication of effort without any thought given to their implications for transfers of individually-identifiable information. Does 15 U.S.C. 638, for example, "authorize" the SBA to transfer information to the FBI? Is such an authorization really necessary?

7 U.S.C. 16: The Secretary of Agriculture may co-operate with any department or agency of the federal government or any state agency (1922)

7 U.S.C. 1607: The Secretary of Agriculture is broadly authorized to co-operate with any department or agency of the federal government or with the states in carrying out his duties in regard to seeds (1939)

7 U.S.C. 1624: The Secretary of Agriculture is given general powers of co-operation with state, federal, and private entities in carrying out his duties on the marketing of agricultural products (1946)

15 U.S.C. 638: The Small Business Administration is authorized to co-operate with federal agencies in carrying out programs for the assistance of small businesses (1958)

16 U.S.C. 590: The Secretary of Agriculture may receive co-operation of any other federal agency in carrying out his duties concerning soil conservation (1935)

29 U.S.C. 527: The Secretary of Labor is authorized to co-operate with other agencies in carrying out his duties concerning labor-management reporting (1959)

30 U.S.C. 556: The Secretary of the Interior is authorized to co-operate with any person or agency, state or federal, in carrying out his duties concerning coal mine fires (1954)

42 U.S.C. 1857: HEW (now EPA) authorized to co-operate with other federal agencies and private organizations concerning air pollution control (1955)

42 U.S.C. 3756: LEAA is authorized to co-operate with the Department of Justice and other agencies

I A(2)

These statutes are concerned with general duties and possibilities of information sharing imposed by statute. They should be distinguished from statutes imposing general duties of co-operation and co-ordination but not mentioning information sharing explicitly.

It is interesting and probably significant that the mandatory language is generally accompanied by a fairly narrowly defined substantive problem thought to warrant the transfer that does not contemplate the *use* of the information in a way that could be detrimental to the subject of the information.

Although perhaps not technically within the scope of this grouping, 44 U.S.C. 3501 was included because it could conceivably be construed to condone, if not authorize, general information sharing of all sorts among federal agencies. Indeed, if 44 U.S.C. 3501 is not limited to statistical tabulations, it may be the answer in part to the problems noted concerning a lack of consistency or general overall constraints and directions concerning transfer of information between agencies: it may indicate that interagency co-operation and transfer is thought and desired by Congress to be the rule rather than the exception. Note also 44 U.S.C. 3507, which gives OMB extensive power to compel interagency transfers: by what standards is not clear, but see 44 U.S.C. 3508. Compare 12 U.S.C. 1141h.

2. U.S.C. 166: Any department or agency shall furnish such books, papers, documents, memoranda to the Congressional Research Service as the Service deems necessary to perform its task of informing Congress (1946)

4 U.S.C. 144: Heads of agencies shall co-operate with the General Services Administration in its collection of papers of territories from which the U.S. was formed by permitting access to records desired necessary by the Administration (1970)

5 U.S.C. 2954: Any executive agency is directed to supply to the Committee on Government Operations of either the Senate or the House any documents within the jurisdiction of the Committee when requested by 7 members of the Committee (1966)

5 U.S.C. 4113: General duty of all agencies to transfer to the Civil Service Commission the names of employees, training received, positions held, and promotions (1966)

5 U.S.C. 8193: Federal departments and agencies directed to furnish the Secretary of Labor information necessary to carry out his duties concerning compensation benefits due injured or dead law enforcement officials (1968)

7 U.S.C. 172: Secretary of Agriculture given wide power to draw on other agencies for information concerning a program for production of rubber plants (1942)

7 U.S.C. 1506: Federal Crop Insurance Corporation may draw information from other agencies to carry out its duties (1938)

8 U.S.C. 1360: Central index of names, addresses, ID information and social security numbers of aliens open to security agents and Attorney General, information from other agencies for this file may be transferred when the Attorney General requests (1952)

12 U.S.C. 1095: The Fair Credit Administration may request from the FDIC, the Comptroller of Currency, the Federal Reserve, and the executive departments of government information relating to the condition of an institution to which it has made or is contemplating making a loan (1916)

12 U.S.C. 1141h: President may by executive order direct any agency to transfer to Fair Credit Administration any information relevant to its activities except that classed as confidential (1929)

12 U.S.C. 1442: The Federal Home Loan Bank may request from the Treasury, Comptroller of Currency, and the Federal Reserve any information relating to institutions with which the Bank has done or is contemplating doing business; banks asking for advances from the Home Loan Bank must consent to this transfer in advance (1932)

12 U.S.C. 1723a: The Government National Mortgage Association and the Federal National Mortgage Association may draw on any executive agency for information necessary to carry out their duties (1934)

12 U.S.C. 1725: The Federal Savings and Loan Insurance Corporation may draw on any agency, department, etc. for information necessary to carry out its duties (1934)

12 U.S.C. 1749 bbb-18: Secretary HUD given wide power to draw on other agencies for transfer of information to HUD (1934)

13 U.S.C. 6: The Secretary of Commerce may call on any department or office of the government for information pertinent to the census (1954)

15 U.S.C. 278g: The Secretary of Commerce may get information from any federal department or agency concerning fire safety and prevention (1907)

15 U.S.C. 634: Small Business Administration given power to draw on other agencies, departments, etc. for any information necessary to carry out its duties (1958)

16 U.S.C. 4601–1: The Secretary of the Interior may obtain information, data and reports from other departments and agencies, concerning outdoor recreation progress (1963)

16 U.S.C. 797: Departments and agencies of the Federal Government are directed to furnish the Federal Power Commission such records, papers, and information as may be required by the Federal Power Commission concerning the cost of licensed projects (1920)

19 U.S.C. 1334: The Federal Trade Commission and other agencies and departments are directed to co-operate with the Tariff Commission, and shall submit all books, papers, records, information to the commission when directed by the President (1930)

22 U.S.C. 2575: The President shall establish procedures for information sharing between the Defense Department, the AEC, NASA, and other agencies with the U.S. Arms Control and Disarmament Agency (1961)

28 U.S.C. 624: The Supervisory Board of the Federal Judicial Center may require from any department, agency, or independent instrumentality any information it deems necessary to carry out the functions of the Federal Judicial Center (1967)

40 U.S.C. 71d: The National Capitol Planning Commission may request information necessary to carry out its planning activities from other agencies: other agencies authorized to request information from National Planning Comm'n (1924)
42 U.S.C. 257: Surgeon General may furnish to a Commissioner of the District of Columbia the names, addresses, and other pertinent information on addicts from the District of Columbia who voluntarily commit themselves for treatment (1956)
42 U.S.C. 1962b–4: A river basin commission may get information from any agency necessary to carry out its statutory duties (1965)
42 U.S.C. 3187: A regional action planning commission may draw information from any agency, department, etc. to carry out its duties (1965)
42 U.S.C. 3211: The Secretary of Commerce is authorized to request from any executive department, bureau agency, etc. such information as is necessary to carry out his duties concerning economic development (1965)
42 U.S.C. 3332: The Secretary of Commerce is authorized to call on other federal agencies to supply statistical data, reports, etc. necessary to carry out its responsibilities concerning areawide development (1966)
42 U.S.C. 3332: Secretary of HUD may request information concerning area-wide development from all agencies concerned with area-wide development to coordinate programs (1966)
42 U.S.C. 3761: The Law Enforcement Assistance Administration may draw such information from other agencies, departments, etc. as it deems necessary to carry out its responsibilities under the Act. (1968)
42 U.S.C. 4304: The Cabinet Committee on Opportunities for Spanish Speaking People may draw from any agency, department, etc. such information as it needs to carry out its statutory duty (1969)
42 U.S.C. 4305: The Advisory Committee on Intergovernmental Relations is authorized to require from any federal department or agency such information as it deems necessary to carry out its functions (1969)
44 U.S.C. 2906: The Administrator of the General Services Administration may inspect or survey the records of any federal agency and make surveys of records management and records disposal (1968)
44 U.S.C. 3501: Information collected that is tabulated by federal agencies shall be tabulated in such a manner as to maximize its usefulness to other agencies (1968)
44 U.S.C. 3507: The Director of the Bureau of the Budget (now OMB) may require a federal agency to make available to another federal agency information obtained from any person; exempted are the IRS, the Comptroller of the Currency and others (1968)
46 U.S.C. 1289: The Secretary of Commerce may draw from any agency, department, etc. such information as he needs to carry out his duties on war risk insurance on ships (1936)
49 U.S.C. 1537: The Secretary of Commerce may draw from any agency such information necessary to carry out his duties on war risk insurance on airplanes (1958)
50 U.S.C. App 1986: The Attorney General may call on any federal department or agency for information necessary for the settlement of American Japanese evacuation claims (1958)

I A(3)

These statutes are grouped together primarily because the agency that requests the information in the first instance appears to be the sole arbiter of the range and classification of the information it may acquire. It is interesting to note that most of these wide-ranging powers are centered on areas which are in themselves fairly narrow and easily defined, and this may act as some check in itself. It is not clear whether, or under what conditions, one agency may refuse the request of another under these statutes, should an agency so desire because, for example, the information sought was obtained under a pledge of "confidentiality." Would honoring a request in the face of such a statute be "authorized by law" within the meaning of 18 U.S.C. 1905, the general criminal provision prohibiting disclosure of confidential information unless authorized by law? Note that there seems to be no means for an agency to enforce a proper request against a recalcitrant agency unless OMB would agree to force the transfer under 44 U.S.C. 3507. I would suspect that these may in fact be moot issues, and whatever information is requested, it is routinely handed over. Nonetheless, it raises interesting issues for the inquiry in general, namely:

(1) Who should determine the propriety of the transfer in the first instance?
(2) How may restrictions or mandates to transfer be enforced among agencies?
(3) If agencies show a reluctance to police themselves in regard to (2), how may they be encouraged to do so?

13 U.S.C. 6: The Secretary of Commerce may call on any other federal agency for information pertinent to the census (1954)
15 U.S.C. 278g: Federal departments and agencies directed to furnish the Secretary of Commerce such information as he deems necessary to carry out his duties concerning fire safety and prevention (1907)
16 U.S.C. 797: All agencies directed to furnish the F.P.C. such information as the F.P.C. may require in determining the cost of the licensed projects (1920)
28 U.S.C. 624: The Supervisory Board of the Federal Judicial Center may require such information as it deems necessary to carry out the functions of the Federal Judicial Center from any department or agency (1967)
31 U.S.C. 21: Under regulations prescribed by the President every department or agency shall furnish the Bureau of the Budget (now OMB) any information the Bureau may require (1921)
42 U.S.C. 3211: The Secretary of Commerce is authorized to request from any executive department, bureau or agency the information and statistics necessary to carry out his duties concerning economic development (1965)
42 U.S.C. 3332: The Secretary of Commerce is authorized to call on other federal agencies to supply such statistics, data, reports, and other matter as he deems necessary to carry out his responsibilities concerning areawide development (1966)
42 U.S.C. 3761: The LEAA is authorized to request any federal agency or department to supply such statistics or data as the LEAA deems necessary to carry out its duties (1968)
42 U.S.C. 4305: The Advisory Committee on Intergovernmental Relations is authorized to require from any federal department or agency such information as it deems necessary to carry out its functions (1969)

I B(1)

These statutes are concerned with the sharing of information between agencies and specifically require the consent of the transferring agency before information can be given to an agency which requests it. While the restraint does not appear to be very great, it is nevertheless interesting that the transferring agency is given a chance to interpose its discretion before the information is transferred. Presumably this could allow the transferring agency to impose restrictions on the transfer of information not otherwise provided by statute.

7 U.S.C. 1506: Federal Crop Insurance Agency may draw from any agency information necessary to carry out its duties, but the information may be transferred only with the consent of the transferring agency (1938)
12 U.S.C. 1723a: The Government National Mortgage Association and the Federal National Mortgage Association may draw on any executive agency for information necessary to carry out their duties, but the information shall be transferred only with the consent of the transferring agency (1934)
12 U.S.C. 1725: The Federal Savings and Loan Insurance Corporation may draw on any agency, department, etc. for information necessary to carry out its statutory duties, but such information is transferred only on the consent of the transferring body (1934)
12 U.S.C. 1749bbb–18: The Secretary of HUD is given wide power to garner information from other agencies; generally the transferring agency must consent first except in areas under HUD's jurisdiction then the information shall be transferred to the extent allowed by law (1934)
15 U.S.C. 634: The Small Business Administration may get information from other agencies necessary to carry out its statutory duties, but information shall be transferred only after transferring agency consents (1958)
46 U.S.C. 1289: The Secretary of Commerce may draw on any agency, department etc. for such information as it needs to carry out its duties as war risk insurer of ships; the information is transferred only with the consent of the transferring agency (1936)
49 U.S.C. 1537: The Secretary of Commerce may draw on any agency, department, etc. for such information as is necessary to carry out its duties as war risk insurer of airplanes, but the information is transferred only on the consent of the transferring agency (1958)

I B(2)

These statutes are concerned with qualifications on sharing of information between agencies. Each directs that the information shall be transferred to the extent allowed by law. Presumably this requirement refers to specific prohibitions in statutes directly concerned with the transferring agency. In contrast to the language of statutes which indicate that information is to be transferred on the consent of the transferring agency, these statutes seem to indicate a more mandatory and complete power to compel transfers.

12 U.S.C. 1749 bbb-18: Secretary of HUD given broad powers to draw on other agencies for information, generally the transferring agency must consent first except in areas of HUD's jurisdiction—then information shall be transferred to the extent allowed by law (1934)

29 U.S.C. 527: Other agencies are directed to co-operate with the Secretary of Labor in carrying out his duties concerning labor-management relations to the extent permitted by law (1959)

29 U.S.C. 668: The Secretary of Labor shall have access to agency records concerning occupational safety unless required by executive order to be kept secret in the interests of national defense and foreign policy (1970)

42 U.S.C. 3187: A regional planning commission may draw such information as it needs from any agency or department to the extent limited by law (1965)

42 U.S.C. 3761: The Law Enforcement Assistance Administration shall draw from other agencies, depts., etc. such information as it deems necessary to carry out its responsibilities under the act, the transfer is to the extent limited by law (1968)

42 U.S.C. 4305: The Cabinet Committee as Opportunities for Spanish-Speaking People may draw on any agency, department etc. for information to carry out its statutory duties, agencies are authorized to transfer this information to the extent provided by law (1969)

I C(1)

The following statutes either require or empower agencies to make certain information public. A fortiori information available to the public is also available to other agencies. One important point to note in these statutes is the type of information required to be made public as contrasted to the type of information which is seemingly more restricted in its dissemination. While in both cases disclosure of the information may stand to prejudice the individual, information required to be made public may be characterized as generally of a sort whose disclosure yields a clear public benefit (such as disclosure of securities information) while as to information accorded more confidential treatment (such as trade secrets) the potential benefit to the public from disclosure is arguably not so clear.

5 U.S.C. 552: Agencies must make public their organization, rules, proceedings and opinions (1966)

7 U.S.C. 12: Secretary of Agriculture allowed to make public the results on investigations of the efficiency of Boards of Trade and statistical information (1922)

7 U.S.C. 12–1: Secretary of Agriculture may make public the names and addresses of commodity traders when requested by committees of either house of Congress (1922)

15 U.S.C. 77ggg: Applications for trust indenture registration shall be available to the public under regulations prescribed by the Commission (1934)

15 U.S.C. 78x: Persons filing information w/ S.E.C. may object to public disclosure; if the Commission deems the material to be in the public interest it may make it public (1934)

15 U.S.C. 80a–44: Information furnished by investment companies to the S.E.C. shall be made public if the Commission through a variety of devices determines that it is in the public interest to do so (1940)

15 U.S.C. 80b–10: Information furnished by investment advisers to S.E.C. shall be made public unless it is found not to be in the public interest to do so; private persons may raise the public interest issue (1960)

15 U.S.C. 330a: All reports from persons engaged in weather modification to the Secretary of Commerce shall be public (1971)

26 U.S.C. 6103: Income tax forms shall be public records but open to inspection only on order of the President and under rules prescribed by the Secretary of the Treasury (1954)

26 U.S.C. 6104: The requests for exemption from tax exempt organizations shall be open to public inspection, except for material concerning trade secrets, processes, etc., or information that would have adverse effect on the organization (1954)
29 U.S.C. 181: The Department of Labor shall furnish to employers and employees information which may aid in the solving of a labor dispute on their request (1947)
29 U.S.C. 435: Details of labor union organization, names of officials, financial holdings of officials, payments to labor unions by employers shall be public information (1959)
30 U.S.C. 732: Reports from mine operators to the Secretary of the Interior on accidents, injuries and occupational diseases shall be made available for public inspection (1966)
30 U.S.C. 821: Reports from mine operators to the Secretary of the Interior concerning accident investigations may be made available to the public and released to interested persons (1969)
42 U.S.C. 263g: Secretary of H.E.W. shall pass on to the public enough of the information furnished him by manufacturers of electronic products concerning details of products likely to cause injury to comply with the purposes of the statute (1944)
42 U.S.C. 2454: All information obtained by NASA shall be available for public inspection except that which is withheld by statute and that which is classified (1958)
46 U.S.C. 927: The collector of customs on the request of any person shall disclose the owners of a vessel, their interest therein and the bill of sale of a vessel 1920)
47 U.S.C. 412: Schedules, charges, and other documents filed with FCC by carriers of wire communications, etc. to be kept as public records (1934)
49 U.S.C. 1504: Information disclosed by air carriers to FAA; carriers may object to public disclosure, and will be withheld if FAA determines not in the public interest (1958)

I C(2)

This section isolates general exceptions to the statutes in the preceding section dealing with the power of a duty of an agency to make certain information public. The general pattern shows that trade secrets and business processes are the items most exempted from public revelation, thus indicating that Congress (and certainly business lobbies) generally consider this sort of information to be "sensitive." Note especially 15 U.S.C. 330a, expressly authorizing interagency transfers of "confidential" information.

5 U.S.C. 552: Agencies in general shall make public their organization, rules, proceedings, opinions, except that no trade secrets shall be disclosed nor personnel records or procedure (1966)
7 U.S.C. 12: Secretary of Agriculture allowed to make public results of investigations of the efficiency of Boards of Trade except that can't reveal any person's business transactions, trade secrets, or names of customers (1922)
15 U.S.C. 77ggg: Applications for trust indenture registration are to be made available to public except that collateral material may be disclosed only to the Attorney General (1934)
15 U.S.C. 78x: The S.E.C., can't disclose publicly trade secrets; also any person who objects to public disclosure may object, but if the Commission deems it to be in the public interest it may be made public anyway (1934)
15 U.S.C. 80a–44: Information furnished by investment companies shall be made public if the S.E.C. through a variety of devices determines that it is in the public interest to do so (1940)
15 U.S.C. 80b–10: Information furnished by investment advisers to S.E.C. shall be made public unless found not to be in the public interest, private persons may raise the issue; can't disclose however that an investigation is underway or results of an investigation or examination (1960)
15 U.S.C. 330a: Reports furnished from persons engaging in weather control to the Secretary of Commerce shall be made public except for information included in 18 U.S.C. 1905, but that information shall be disclosed to other departments or agencies for official use on their request and to the public if necessary to protect their health and safety & in judicial proceedings (1971)
26 U.S.C. 6103: Income tax forms filed by taxpayers shall be public records but open to inspection only on order of the President and under rules and regulations prescribed by the Secretary of the Treasury (1954)

26 U.S.C. 6104: Applications for tax exempt status from tax exempt organizations shall be open to public inspection, but on request the Secretary may withhold information related to trade secrets and processes, or information that would have an adverse effect on the organization (1954)

29 U.S.C. 181: The Department of Labor may furnish on request to employers and employees all data which may aid in the solving of a labor dispute except information submitted in confidence (1947)

42 U.S.C. 263g: Secretary shall disclose to public enough of the information furnished him by manufacturers of electronic products of defects likely to cause injury to carry out the purposes of the act however he shall not disclose trade secrets or other things referred to in 148 U.S.C. 1905 unless necessary to carry out the policy of the act (1944)

42 U.S.C. 2454: All information obtained by NASA shall be available for public inspection except that which is required to be withheld by statute and that which is classified (1958)

47 U.S.C. 412: Schedules, charges, and other documents filed by carriers of wire communications with the FCC to be kept as public records except such things as the FCC decides to keep confidential to the public interest (1934)

49 U.S.C. 1504: Any person may object to disclosure of information disclosed to the FAA and the information shall be withheld if the board or administrator determines it will hurt the person involved and is not in the public interest (1958)

ID

The following statutes deal explicitly with the possibility of sharing of information between state and federal governments. A great number of other statutes impose duties of co-operation with states on federal agencies in general terms. Conceivably these general statutes could be construed to allow information sharing between state and federal agencies. These statutes are too numerous and too vague, however, to be of much use without an extensive search of C.F.R. to use if information transfer procedures have been established.

5 U.S.C. 8506: Federal agencies may transfer to the states personnel information concerning compensation, period of employment and reasons for termination of federal employees for purposes of unemployment compensation (1966)

5 U.S.C. 8523: Federal government may transfer to the states information as to compensation, period of employment, etc. for purposes of unemployment compensation for ex-servicemen (1966)

7 U.S.C. 515e: The Department of Agriculture may transfer to the states any tobacco information, statistics, etc. as the Secretary deems appropriate to aid the states (1936)

7 U.S.C. 610: The Department of Agriculture may transfer information to the states received under 7 U.S.C. 60Fd (information from parties subject to restrictions concerning agricultural commodities) to the extent that it is relevant to the state agency's jurisdiction provided that the information is kept in confidence by all offices and employees of the state agency and disclosed only in a suit or administrative hearing (1935)

42 U.S.C. 242: The Surgeon General may co-operate with the states to help them solve their narcotic drug problem (1970)

42 U.S.C. 644: At the request of a qualified state agency the Secretary of HEW, as receipt of a list of names, shall give the state a list of persons involved in work incentive plans (1968)

42 U.S.C. 1306: The Secretary of HEW on Labor may transfer social security information concerning an individual's name and address and most recent employer to the states if the individual is under child support obligation in that state (1935)

II. STATUTES RESTRICTING TRANSFERS OF INFORMATION

IIA(1)

These statutes deal with restrictions placed on transfers of information either because it is classified as "confidential" or is cross referenced to 18 U.S.C. 1905, which is the most general criminal statute prohibiting disclosure of information:

Whoever, being an officer or employee of the United States, or of any department or agency thereof, publishes, divulges, discloses or makes known in any manner not authorized by law any information coming to him in the course of his employment or official duties . . . which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data . . . of any person, firm, partnership, or

association . . . shall be fined not more than $1,000 or imprisoned for not more than one year, or both; and shall be removed from office or employment.

The classification of "confidential" is also important in light of 44 U.S.C. 3508, which extends the confidentiality controls to agencies receiving information from the agency to which the original restriction applied:

(a) If information obtained in confidence by a Federal Agency is released by that agency to another Federal agency, all the provisions of law including penalties which relate to the unlawful disclosure of information apply to the officers and employees of the agency to which the information is released to the same extent and in the same manner as the provisions apply of officers and employees of the agency which originally obtained the information.

It is unclear whether "confidentiality" refers only to making the information public, or extends to interagency transfers as well.

For the most part there is a close identity between information classed as confidential without reference to 18 U.S.C. 1905, and the business and trade information protected by 18 U.S.C. 1905.

5 U.S.C. 552: Agencies are required to make public a description of their organization, their proceedings, substantive rules, opinions, and statements of policy except items made secret by executive order, trade secrets, commercial and financial information that is privileged or confidential plus several other exceptions (1967).

7 U.S.C. 12: The Secretary of Agriculture may publicize the results of investigations of Boards of Trade except that data and information which would separately disclose the business transactions, trade secrets, or names of customers of any person (1922).

7 U.S.C. 135b: Data from distributors of economic poisons submitted to a committee on economic poisons challenging the classification of a substance as an economic poison shall be considered confidential (1947).

7 U.S.C. 472: Data concerning quality and grades of cotton submitted from cotton mills, warehouses, etc. to the Secretary of Agriculture shall be considered confidential (1927).

7 U.S.C. 608d: Records, reports, data, etc. submitted by parties subject to restrictions concerning agricultural commodities to the Secretary of Agriculture shall be kept in confidence (1933).

7 U.S.C. 610: Same information in 608d being transferred from Federal government to state agencies, states required to keep confidential in the same manner (1935).

7 U.S.C. 1373: Information furnished by warehousers, processors, and common carriers of various commodities furnished to the Secretary of Agriculture shall be kept confidential by officers and employees of the department and disclosed only in a suit or administrative hearing (1938).

7 U.S.C. 2105: Reports, records, data, etc. submitted from cotton growers, handlers, etc. to the Cotton Board shall be kept confidential by Department of Agriculture (1966).

8 U.S.C. 1202: Information obtained from aliens applying for visas concerning identifying marks, names, address, arrest record, purposes, languages used, etc. shall be kept confidential (1952).

8 U.S.C. 1304: Information obtained from aliens in the country such as fingerprint, date of entry, purpose, arrest record shall be kept confidential (1952).

10 U.S.C. 7303: Information concerning results of private experiments in the Model Basin are confidential (1956)

12 U.S.C. 1091: Reports on the condition of national banks furnished by the Comptroller of Currency to the Federal Intermediate Credit Bank are to be for the confidential use of the Intermediate Credit Bank (1916)

12 U.S.C. 1141h: Information classed as confidential excepted from general power of transfer from any agency to the Fair Credit Administration by executive order (1929)

13 U.S.C. 302: The Secretary of Commerce is given power to regulate confidentiality of information furnished the Census Bureau by regulation (1962)

15 U.S.C. 176a: Information concerning industries and markets furnished by individuals, corporations and firms to the Bureau of Foreign and Domestic Commerce is to be confidential (1938)

15 U.S.C. 330a: All reports from persons engaging in weather modification to the Secretary of the Interior shall be made public except for the matter covered in 18 U.S.C. 1905 which shall only be released to other federal departments or agencies on their request for their official use, or in judicial proceedingss, or when necessary to protect the public health and safety (1971)

15 U.S.C. 1193: Information furnished by manufacturers and persons dealing in flammable items to the Secretary of Commerce concerning flammability of products, etc. shall be considered confidential; extends only to trade secrets and other matter enumerated in 18 U.S.C. 1905 (1953)

15 U.S.C. 1401: Information furnished by manufacturers of motor vehicles to Secretary of Commerce on compliance with safety standards that is a trade secret or otherwise enumerated in 18 U.S.C. 1905 shall be considered confidential for purposes of 18 U.S.C. 1905 (1966)

18 U.S.C. 1902: Prohibits premature disclosure of information that might affect the price of agricultural goods; $10,000/10 years (1948)

18 U.S.C. 1904: Prohibits unauthorized disclosure of information on future action of Reconstruction Finance Corporation that might affect the value of securities: $10,000/5 years (1948)

21 U.S.C. 346a: Information concerning tolerance limits for poisons in pesticides submitted from persons challenging proposed tolerance limits to Administrator of EPA shall be confidential until publication of the proposed regulation (1938)

26 U.S.C. 7213: Prohibits disclosure of income tax return information except as provided by law; cross referenced to 18 U.S.C. 1905 which makes confidential business processes, etc. (1954)

29 U.S.C. 181: Excepts from data that Department of Labor may furnish employers and employees in the solving of a labor dispute any specific information submitted in confidence (1947)

30 U.S.C. 872: Maps of coal mines submitted by coal operators to Secretary of H.E.W. shall be kept as confidential except so far as is necessary to carry out purposes of the chapter (1969)

33 U.S.C. 1160f: Information submitted by alleged water polluters concerning the character and control of pollution to Secretary of Interior, trade secrets, etc. considered confidential for purposes of 18 U.S.C. 1905 (1966)

35 U.S.C. 122: Information submitted by applicants for patents to the Patent Office to be kept in confidence (1952)

38 U.S.C. 3301: Information submitted from VA benefits claimants to VA concerning claims shall be considered privileged and confidential (1958)

42 U.S.C. 260: Records of addicts who voluntarily commit themselves for treatment are to be kept confidential and not divulged by Surgeon General, can't be used against them in court (1956)

42 U.S.C. 263g: Excepts from public disclosure of defects likely to do injury in electronic products any trade secret or other things referred to in 18 U.S.C 1905 unless necessary to carry out policy of act (1944)

42 U.S.C. 263i: Excepts from public disclosure of reports, etc. concerning radiation safety of electronic products any trade secrets or other matter mentioned in 18 U.S.C. 1905 (1944)

42 U.S.C. 1857d: Information from alleged air polluters concerning the nature of pollution and pollution controls given to Secretary of H.E.W. (now E.P.A.), trade secrets, etc. are considered confidential for purposes of 18 U.S.C. 1905 (1955)

42 U.S.C. 1857f–6: Reports from manufacturers of autos to determine compliance w/emission control standards, trade secrets & other matter mentioned in 18 U.S.C. 1905 are not to be disclosed (1955)

42 U.S.C. 1857f–6c: Data concerning fuel additives submitted by manufacturers of water fuels, trade secrets & other matter mentioned in 18 U.S.C. 1905 are not to be disclosed (1955)

42 U.S.C. 2000g–2: Information submitted to the Community Relations Service with the understanding that it is to be in confidence prohibited from disclosure to public (1964)

42 U.S.C. 2181: Information required to be submitted by inventors of inventions relating to atomic energy to be kept in confidence and not given out without permission of owner (1946)

42 U.S.C. 2723: Excerpts confidential information from transfer of training records of Job Corps trainees from Director of Job Corps to Department of Labor (1967)

43 U.S.C. 1398: Witnesses before the Commission on Public Land Law Review may submit information on a confidential basis which is not to be made public (1964)

44 U.S.C. 3508: Information supplied to an agency as confidential can't be transferred between agencies w/o consent of original supplier; excepts statis-

ties on situation which agencies would have concurrent power to gather information (1968)

49 U.S.C. 1681: Material furnished by gas pipe line owners and operators to the Secretary of Transportation to determine compliance w/regulations, trade secrets and material in 18 U.S.C. 1905 shall be considered confidential for purposes of that statute (1968)

50 U.S.C. App. 643a: No publication of any books and records produced in the course of an inspection or audit by the War Production Board which the Chairman believes to be confidential or anything for which a request for confidentiality is made unless national interest requires otherwise (1942)

50 U.S.C. App. 1152: No publication of any records submitted by defense contractors to President which are required to enforce emergency contracting procedures which President deems confidential or which has been requested to be treated as confidential unless national interest requires otherwise (1940)

50 U.S.C. App. 2406: No publication of any data submitted by exporters to determine compliance with export control act which is deemed confidential or which has been requested to be treated as confidential unless national interest requires otherwise (1972)

II A(2)

These statutes contain *exceptions* to restrictions placed on transfers of information because it is classed as "confidential" or is restricted because of 18 U.S.C. 1905. It was hoped that isolation of the exceptions would clarify some of the ambiguities which attend the use of "confidential" in referring to information. Some of the exceptions seem to imply that the confidential classification is a restriction only against making information public—see especially 15 U.S.C. 330a—while others imply a limit on the transfer of information among agencies. Note especially 21 U.S.C. 1175, an example of what Congress can do in this area when it tries.

5 U.S.C. 552: Agencies are required to make public a description of their organization, their proceedings, substantive rules, opinions, and statements of policy except items made secret by executive order, trade secrets, commercial and financial information that is privileged or *confidential* plus several other exceptions (1967)

7 U.S.C. 12: The Secretary of Agriculture may publicize the results of investigations of Boards of Trade except that data and information which would separately disclose the business transactions, trade secrets, or names of customers of any person (1922)

7 U.S.C. 135b: Data submitted by manufacturers of economic poisons challenging classification of a substance as an economic poison shall be considered confidential except that the advisory committee to whom data is submitted may use it in consultation with the E.P.A. (1947)

7 U.S.C. 1373: Information furnished by warehousers, processors, and common carriers of various commodities furnished to the Secretary of Agriculture shall be kept confidential by officers and employees of the department and disclosed only in a suit or administrative hearing (1938)

7 U.S.C. 2105: Information submitted by cotton growers, handlers, etc. to Cotton Board is to be kept in confidence except publication may be made of general statements and the names of violators (1966)

8 U.S.C. 1202: Information submitted by aliens applying for visas concerning name, address, purpose, arrest record, identifying marks are to be kept confidential except it may be used for enforcement of the immigration laws (1952)

10 U.S.C. 7303: Information of results of private experiments in the Model Basin are to be kept confidential and may not be disclosed without the consent of the person for whom they were made (1956)

15 U.S.C. 330a: All reports from persons engaging in weather modification to the Secretary of the Interior shall be made public except for the matter covered in 18 U.S.C. 1905 which shall only be released to other federal departments or agencies on their request for their official use, or in judicial proceedings, or when necessary to protect the public health and safety (1971)

15 U.S.C. 1193: Information submitted by manufacturers of flammable items on flammability shall be confidential for purposes of 18 U.S.C. 1905, except that it can be disclosed to officers and employees carrying out the provisions of this chapter (1953)

18 U.S.C. 1906: Prohibits bank examiners from disclosing the names of borrowers or the collateral for loans to anyone other than the officers of the bank without express permission to do so in writing from the Comptroller of Currency or

Federal Reserve Board of Governors or the bank's officers, except when ordered to do so by a court or Congress; $5,000/1 year (1948)

18 U.S.C. 1907: Prohibits farm credit examiners from disclosing the names of borrowers of Federal land banks, etc., to anyone other than the officers of the examinee without the express permission in writing of the Land Bank Commissioner or the examinee, except when ordered to do so by a court or Congress; $5,000/1 year/loss of job (1948)

18 U.S.C. 1908: Prohibits National Agricultural Credit Corp. examiners from disclosing names of borrowers of any organization examined to anyone other than officers of the examinee without the express permission in writing of the Comptroller of Currency or the examinee, except when ordered to do so by a court or Congress; $5,000/1 year/loss of job (1948)

13 U.S.C. 214: Prohibits Census employees from disclosing any Census info without written permission from an authorized employee or officer of the Department of Commerce; $1,000/2 years (1954)

21 U.S.C. 346a: Information submitted challenging proposed tolerance limits for poisons in pesticides shall be confidential until the proposed regulation is published (1938)

21 U.S.C. 1175: Records of any patient treated under drug abuse prevention program is confidential, but may be disclosed in very narrow circumstances: with patients consent, to doctors and government personnel giving patient benefits: without consent, to medics in an emergency, in statistical form, or on court order on a showing of good cause—which is limned in some detail (1972)

30 U.S.C. 872: Map of coal mine submitted by coal mine operator to Secretary of HEW shall be kept confidential except as it is necessary to carry out the purposes of this chapter (1969)

35 U.S.C. 122: Information on applications for patents to be kept in confidence and can't be disclosed without consent of owner or in compliance with an act of Congress, or under such special circumstances as determined by the Commission (1952)

38 U.S.C. 3301: Information pertaining to claim by a VA benefits claimant to be considered confidential and privileged and no disclosure made *except* to the claimant in certain circumstances, in a court proceeding, to any agency or department which requests it, and if there is an inquiry into the compensation received by a claimant (this is an independent ground) (1958)

42 U.S.C. 260: Records of addicts who voluntarily commit selves are to be confidential except that in the case of those from District of Columbia Surgeon General may give a D.C. Commissioner the name and address as well as any other information relevant to rehabilitation; X-ref to 42 U.S.C. 257 for operative language (1956)

42 U.S.C. 263g: Notice of defects in electronic products likely to cause injury shall be made public unless it's a trade secret or otherwise mentioned in 18 U.S.C. 1905—then it shall be disclosed only as far as it is necessary to carry out the policy of the act (1944)

42 U.S.C. 1857f–6: Reports from auto manufacturers to determine compliance with emission control standards, no disclosures of trade secrets or matter in 18 U.S.C. 1905 except to officers and employees at agency and committees of Congress (1955)

42 U.S.C. 1857f–6c: Reports from manufacturers of motor fuels concerning fuel additives, no disclosure of trade secrets or material listed in 18 U.S.C. 1905 except to Secretary and employees of agency and to Committees of Congress (1955)

42 U.S.C. 2181: Special reports required of inventors of inventions related to atomic energy to be kept in confidence and not to be given out without the authority of the owner unless to carry out an Act of Congress or in special circumstances as determined by the Commissioner of Patents (1946)

49 U.S.C. 1681: Information supplied by gas pipeline owners and operators to Secretary of Transportation to determine compliance with rules and restrictions, trade secrets and other matters in 18 U.S.C. 1905 shall be considered confidential for purposes of that statute, except that disclosure is allowed to members of the agency and committees of Congress (1968)

II B(1)

These statutes try to limit the dissemination of information furnished by individuals by providing that it may be used for statistical purposes only. Thus, aggregate information can be passed to and used by other entities, but the individual is insulated by the anonymity of statistics. There is some question,

however, as to whether the limitation extends to all extra-agency use or just to information made available to the public. The statutes themselves give little help on this point, unless the designation of the information as "confidential" can be said to extendt the restriction to interagency transfers.

7 U.S.C. 472: Information concerning grades and quality of cotton furnished by cotton mills, warehouses, etc. to the Secretary of Agriculture shall be considered confidential and used for statistical purposes only (1927)

7 U.C.C. 507: Information concerning tobacco on hand plus general data concerning the tobacco industry furnished by tobacco growers, merchants, associations etc. to the Department of Agriculture are to be used for statistical purposes only (1929)

7 U.S.C. 608d: Information furnished by parties concerning agricultural commodities subject to restrictions to Department of Agriculture and shall be kept confidential by all officers and employees of Agriculture, however agency can publish general statistics (1933)

7 U.S.C. 955: Information concerning quantity of peanuts and oil processed and shipped furnished by those manufacturing, selling, and warehousing peanuts and peanut products to the Department of Agriculture should be used only for statistical purposes (1936)

13 U.S.C. 9: Information obtained through census can be only used for statistical purposes (1954)

15 U.S.C. 176a: Information concerning industries and markets furnished by individuals, corporations, and firms to the Bureau of Foreign and Domestic Commerce shall be confidential and used only for statistical purposes (1938)

42 U.S.C. 242c: Information obtained for statistical studies of national health needs cannot be used for non-statistical purposes except to extend provided for in regulations by HEW Secretary *and* with subject's consent

II B(2)

These statutes are a subgroup of the statutes which allow information to be used only for statistical purposes since they include the statistical purposes requirement, and also require that no publication shall be made wherein individuals may be identified. While the requirement may be redundant it presumably emphasizes the protection to be accorded individuals by the assurance of statistical anonymity.

7 U.S.C. 507: Information concerning tobacco on hand plus general information furnished by tobacco growers association, merchants, etc. to the Department of Agriculture shall be used for statistical purposes only and no publication shall be made where any individual may be identified (1929)

7 U.S.C. 955: Information concerning the quantity of peanuts and oil processed and shipped furnished by those manufacturing, selling and warehousing peanuts to the Secretary of Agriculture shall be used for statistical purposes only and no publication may be made wherein individuals may be identified (1936)

13 U.S.C. 9: Information furnished through census is to be used only for statistical purposes; the Bureau can't make any publication wherein individuals are identified (1954)

II B(3)

These statutes deal with exceptions to the limitation that information may be used for statistical purposes only.

7 U.S.C. 608d: Information furnished by parties subject to restrictions concerning agricultural commodities to the Department of Agriculture shall be kept confidential except that they may be disclosed in a suit or administrative hearing, or may publish general statistics and names of people violating agreements (1933)

13 U.S.C. 9: Information furnished in course of census can only be used for statistical purposes, however can furnish geneological data and certain other special statistics (1954)

42 U.S.C. 242c: Information obtained for statistical studies of national health needs cannot be used for non-statistical purposes except to extent provided for in regulations by HEW Secretary *and* with subject's consent (1970)

II C(1)

These statutes deal with information furnished to agencies in which the statutes seems clearly to indicate that the information is to be used only within the agency to which it is furnished. They should probably be contrasted with other statutes whose restrictions on the use of the information are less clear.

The most interesting, but unsurprising, aspect of these statutes is the type of information concerned: in almost every instance it is information relating to business or trade.

7 U.S.C. 507: Information on tobacco stocks and general business data from tobacco growers, merchants, warehouses etc. given to Department of Agriculture may be examined only by sworn employees of Department of Agriculture (1929)

7 U.S.C. 608d: Information furnished by parties subject to restrictions vis-a-vis agricultural commodities to the Department of Agriculture is to be kept confidential by all officers and employees of Agriculture and disclosed only in a suit or administrative hearing (1933)

7 U.S.C. 955: Information furnished by those manufacturing, selling, warehousing peanuts and peanut products concerning the quantity of peanuts and oil processed and shipped, to Department of Agriculture can only be examined by sworn employees of the Department of Agriculture (1936)

7 U.S.C. 1373: General business information furnished by handlers of agricultural commodities to Department of Agriculture to be kept in confidence by all officers and employees of Department of Agriculture and disclosed only in a suit or administrative hearing (1938)

7 U.S.C. 2105: Information furnished by cotton growers, handlers, etc. furnished to Cotton Board in administration of statute shall be kept confidential by the Secretary and employees of Department of Agriculture and disclosed only in a suit or administrative hearing (1966)

13 U.S.C. 9: Data derived from census reports is not allowed to be veiwed by anyone outside of census bureau (1954)

15 U.S.C. 79v: Any information furnished by utility holding companies to the S.E.C. that is not public document may not be disclosed outside of the Commission (1935)

22 U.S.C. 987: Personnel records of foreign service officers may be viewed only by the President, Secretary of State, Under Secretary of State, committees of Congress, and under certain circumstances to the officer to whom it relates (1946)

II C(2)

These statutes were grouped together because of a similarity in language which seems to indicate that information received by an agency or other official body is to remain inside of that agency except in certain narrowly defined circumstances—usually orders to transfer the information from some superior authority. In some of the statutes, however, it is unclear as to whether the information shall remain in the agency or is simply not to be made public. Note

7 U.S.C. 135d, though: no question there about interagency transfers.

7 U.S.C. 135d: Unlawful for any person to use formulae of economic poisons furnished by the manufacturers etc. thereof to the EPA for his own benefit or advantage or to disclose the information outside the EPA except to federal agencies or courts (1964)

7 U.S.C. 608d: Information furnished by parties subject to restrictions concerning agricultural commodities to the Secretary of Agriculture to be kept in confidence by all officers and employees of Agriculture and disclosed only in a suit or administrative hearing, however can publish general statistics and the names of people violating agreements (1933)

7 U.S.C. 1373: Information furnished by handlers of agricultural commodities to Secretary of Agriculture to be kept in confidence by all officers or employees of the Department of Agriculture and disclosed only in a suit or adminstrative hearing (1938)

7 U.S.C. 2105: Information furnished by cotton growers, handlers, etc. to the Cotton Board is to be kept confidential by the Secretary and employees of Agriculture and disclosed only in a suit or administrating hearing; publication of general statements and names of violators is allowed however (1966)

15 U.S.C. 79v: Information furnished by utility holding companies to the SEC in the form of non-public documents may not be disclosed outside of the SEC except to the Federal Reserve (1935)

16 U.S.C. 825: Accounts, accounting procedures and other business information furnished by public utilities to the Federal Power Commission may not be divulged except as directed by commissioner or ordered by a court (1920)

42 U.S.C. 1857f-6: Concerns reports to determine compliance with emission control standards furnished by manufacturers of autos; no disclosure of trade

secrets or other matter in 18 U.S.C. 1905 except to officers and employees of agency; can disclose to committees of Congress, through (1955)

42 U.S.C. 1857f–6c: Concerns data concerning fuel additives furnished by manufacturers of motor fuels; no disclosure of trade secrets or other matter listed in 18 U.S.C. 1905 except in the case of members of the agency and committees of Congress (1955)

42 U.S.C. 2181: Special reports filed by inventors of inventions concerning atomic energy are to be kept in confidence and no such information given out without the consent of the owner unless necessary to carry out an Act of Congress in special circumstances determined by the Commissioner of Patents (1946)

49 U.S.C. 1021: Any agent or employee who discloses information provided by freight forwarders to the ICC which comes to him under the statute except as directed by the Commission or a court is guilty of a misdemeanor (1887)

49 U.S.C. 1472: Any agent or employee who discloses information provided by air carriers to the FAA which comes to him under the statute except as directed by the Administration or a court is guilty of a misdemeanor (1958)

II D

These statutes furnish the basis for explicit restraints on information transfer by providing for restrictions on the dissemination of information furnished to an agency by order, or by regulations to be formulated by the agency. It is notable that some of the most personal subjects of the entire search in terms of the type of information concerned were found in this group of statutes, which appear to give a wide latitude to agency discretion. Note 22 U.S.C. 2573 and 31 U.S.C. 1061, both of which contemplate interagency transfers.

7 U.S.C. 2017: Regulations shall be issued providing for the safeguarding of information furnished by retail food stores in applications to participate in the food stamp program (1964)

13 U.S.C. 302: Secretary of Commerce given the power to regulate the confidentiality of census returns by rules, regs. etc. (1962)

15 U.S.C. 77ggg: Applications for trust indenture registration shall be available to the public under regulations prescribed by SEC except as limited by 15 U.S.C. 77uuu (material other than application available only to Attorney General) (1934)

15 U.S.C. 77uuu: SEC may get information from other agencies concerning applications for trust indentures under conditions prescribed by SEC (ambiguity here—other agencies' regulations might be important too) (1934)

21 U.S.C. 872c: AG can authorize withholding of names and characteristics of persons subject to drug research; this authorization shields from process of any kind the names, etc. to the extent of the authorization (1970)

22 U.S.C. 987: Personnel records of foreign service officers may be divulged to the officer to whom the records relate in accordance with regulations (1946)

22 U.S.C. 2575: The President is authorized to establish procedures for the interchange of information between the U.S. Arms Control and Disarmament Agency and Department of Defense, NASA, AEC and other government agencies (1961)

26 U.S.C. 6103: Information on tax returns may be made available on the order of the President and then in compliance with rules and regulations—apparently means made available to anyone President designates (1954)

31 U.S.C. 1061: The Secretary of the Treasury pursuant to regulations may make available to other departments or agencies reports of currency and foreign transactions of individuals (1970) N.B.—is being challenged as unconstitutional

42 U.S.C. 242a: Secretary of HEW may authorize protection of drug use research personal microdata from those not conducting research; immunity from any process to extent of authorization (1970)

42 U.S.C. 1306: Information obtained from registrants and recipients of social security may be disclosed only pursuant to regulations issued by Sec'y of HEW, except that S.S.A. may disclose address of individual and name and address of most recent employer to a state when the individual has child support obligations in that state (1935)

42 U.S.C. 4582: Secretary of HEW may authorize protection of alcohol use research personal microdata from those not conducting research; immunity from all process to extent of authorization (1970)

50 U.S.C. App. 460: The Director of Selective Service is to prescribe rules and regulations for confidentiality of records obtained under the Selective Service Act (1948)

II E(1)

Not all confidential information is so classified in advance by statute. The following are examples of statutes which explicitly recognize that confidentiality may be determined on a case by case basis at the time the information is collected.

29 U.S.C. 181: The Department of Labor may furnish to or request of employers and employees all data which may aid in the solving of a labor dispute except specific information submitted in confidence (1947)

43 U.S.C. 1398: Witnesses before the Commission on Public Land Law Review may submit information on a confidential basis which is not to be made public (1964)

44 U.S.C. 3508: Information supplied as confidential at the time of its taking can't be transferred between agencies without the consent of the party which furnishes the information; does not prohibit transfers of statistics, or or information which the receiving agency could have gotten on its own (1968)

II E(2)

These statutes were grouped together because of similar provisions which give the individual furnishing the information the right to request that it be treated as confidential and/or that it not be disclosed to the public. After such a request has been made, the requesting agency makes an evaluation of the request and may or may not accede to the individual's wishes if certain standards are met. An interesting sidelight is the fact that most of the statutes recognizing this control are part of a general regulatory scheme which compels disclosure of the information in furtherance of its regulatory goals. They raise the possibility that a hearing may be used as a device to control interagency transfer of information. There is a problem in some of the statutes, however, in determining whether the objection is good only to prevent the information from being made public or whether it actually inhibits the transfer of information between agencies.

15 U.S.C. 78m: Information from issuers of registered securities which SEC believes is necessary to protect the public may be required by S.E.C. (and implies that material is to be public) except that in the case of loan disclosures if the person filing so requests, the name of the bank shall not be disclosed (1933)

15 U.S.C. 78x: Covers persons generally filing information with the S.E.C.; no disclosure of trade secrets may be made and persons may raise objections to public disclosure generally; yet if the Commissioner deems the information to be in the public interest he may make it public (1934)

15 U.S.C. 79v: S.E.C. may disclose information obtained from utility holding companies if it is in the public interest; persons may object to disclosure as not in the public interest (1935)

15 U.S.C. 80b-10: Information furnished by investment advisors to the S.E.C. shall be made public unless it is found not to be in the public interest; private persons can raise this issue (1960)

26 U.S.C. 6104: Application for tax exempt status by tax exempt organizations shall be open to public inspection but on request the Secretary may withhold information concerning trade secrets or processes or information that would have an adverse effect on the organization (1954)

49 U.S.C. 1504: Concerns information disclosed to FAA by air carriers pursuant to the requirements of regulation of air carriers; any person may object to disclosure and information shall be withheld if board or administrator determines it will hurt the person involved and is not in the public interest; Committees of Congress may receive information despite objections (1958)

50 U.S.C. App. 643a: Books, documents, etc. produced in the course of an inspection or audit by the War Production Board shall not be published if the information is believed to be confidential or if a request for confidential treatment has been made and the national interest does not require otherwise (1942)

50 U.S.C. App. 1152: Concerns books, records, etc. obtained from defense contractors by President to enforce emergency contracting procedures; the President shall not publish any information which he deems to be confidential or which any person requests to be treated as confidential unless national interest requires otherwise (1940)

50 U.S.C. App. 2406: Concerns information obtained from exporters to determine compliance with the export control act; no disclosure or publishing of information which is deemed confidential or if person requests and withholding is not contrary to the national interest (1972)

II F

These statutes deal with controls placed on state agencies administering welfare programs which are at least partially funded by the federal government. They are unique in that they impose some of the strongest restrictions on the dissemination of information found in the search. If the state aid program is financed by federal funds, each agency must develop safeguards which limit the use of information furnished by applicants and recipients of the aid to only those in the state agency concerned with the direct administration of the program. This raises the question whether this is normal practice in federal agencies in general, related federal agencies such as HEW, or is just an example of a federal double standard.

7 U.S.C. 209: State agency administering food stamp program must develop safeguards which limit access to information provided by applicants for stamps to those directly concerned with administration of the program (1964)

42 U.S.C. 302: State agency administering old age assistance program must develop safeguards which restrict the disclosure of information to those directly concerned with administering the program (1939)

42 U.S.C. 602: State agency administering aid to needy families with children program must develop safeguards which restricts use of information to those concerned with the direct administration of the program (1939)

42 U.S.C. 1202: State agency administering aid to the blind shall make regulations which restrict use of information to those directly administering the program (1939)

42 U.S.C. 1352: State agency administering aid to permanently and totally disabled must provide safeguards that the information is available only to those in direct administration of the programs (1935)

42 U.S.C. 1382: State agency administering aid to aged, blind, disabled, or medical assistance aid must provide safeguards which restrict the use of information to those in direct administration of the program (1935)

42 U.S.C. 1396a: State agency administering medical assistance aid must provide safeguards that insure information is available only to those in direct administration of the program (1935)

II G

For one reason or another those statutes were not placed with any other group. Generally they deal with restrictions on dissemination of information. Note 12 U.S.C. 1829b, the only real "Big Brother" provision produced in the search.

7 U.S.C. 1764: Agricultural attachés shall make available to the Secretary of State and other interested agencies information they have collected concerning foreign markets (1954)

12 U.S.C. 1141j: Penalties for disclosure of confidential information given by Fair Credit Administration to cooperatives, clearing house corporations and similar sorts of marketing utilities in the private sector (1929)

12 U.S.C. 1829b: Insured banks shall furnish the Secretary of the Treasury records on the identity of each person having an account, the identity of each person authorized to sign checks, microfilms of checks and other transactions; the avowed purpose is for criminal, tax, and regulatory matters (1950) N.B.—is being challenged as unconstitutional

15 U.S.C. 717g: Information concerning accounts, accounting procedures and other general business information furnished by natural gas companies to the Federal Power Commission can't be disclosed except as directed by the Commission or a court (1938)

15 U.S.C. 717i: The Commodity Credit Corporation is authorized to use the services, facilities, employees and information of any agency of the federal government and certain enumerated subdivisions of the department of Agriculture (1948)

21 U.S.C. 355: The manufacturers of new drugs sought to be approved for entry into interstate commerce shall forward to the Secretary of H.E.W. information concerning the clinical experiences with the drugs: the Secretary in requesting the information shall observe a due regard for the ethics of the medical profession and the interest of the patients (1962)

21 U.S.C. 257: Manufacturers of drugs containing certain antibiotics shall furnish clinical data to the Secretary of H.E.W.; in requiring the data the Secretary shall observe a due regard for the ethics of the medical profession and the interests of the patients (1962)

45 U.S.C. 362: Information received from claimant by the Railroad Retirement Board shall not be revealed or open to inspection or published in any way to reveal an employee's ID except that information may be disclosed to other agencies involved in administration, claimants, and in other circumstances in which the Board thinks it is in the public interest (1938)

47 U.S.C.: Information furnished by carriers of communication by wire or radio in interstate or international trade to the FCC in the nature of business records etc., shall not be divulged by any officers or employees except as directed by the FCC or by a court (1934)

49 U.S.C. 20: Information furnished by railroads and pipeline carriers to the ICC in the nature of annual reports shall not be disclosed by an examiner or agent unless directed by the Commission or a court (1887)

49 U.S.C. 320: Concerns information furnished by work carriers to the ICC in the form of such periodic reports as the ICC may require; reports concening accidents cannot be admitted in evidence against the water carrier

49 U.S.C. 917: Information disclosed by water carriers to the ICC pursuant to 49 U.S.C. 913 (annual reports concerning business) may not be disclosed by any agent, examiner etc. except as directed by the Commission or a court; penalties provided for unauthorized disclosure (1887)

○