AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

H.R. 220, THE FREEDOM AND PRIVACY RESTORATION ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

H.R. 220

TO AMEND TITLE II OF THE SOCIAL SECURITY ACT AND THE INTERNAL REVENUE CODE OF 1986 TO PROTECT THE INTEGRITY AND CONFIDENTIALITY OF SOCIAL SECURITY ACCOUNT NUMBERS ISSUED UNDER SUCH TITLE, TO PROHIBIT THE ESTABLISHMENT IN THE FEDERAL GOVERNMENT OF ANY UNIFORM NATIONAL IDENTIFYING NUMBER, AND TO PROHIBIT FEDERAL AGENCIES FROM IMPOSING STANDARDS FOR IDENTIFICATION OF INDIVIDUALS ON OTHER AGENCIES OR PERSONS

MAY 18, 2000

Serial No. 106–206

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

71–388 DTP WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
LISA SMITH ARAFUNE, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
HEATHER BAILEY, *Professional Staff Member*
BRYAN SISK, *Clerk*
TREY HENDERSON, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on May 18, 2000	1
Text of H.R. 220	3
Statement of:	
Bovbjerg, Barbara, Associate Director of Education, Workforce, and Income Security Issues, Health, Education, and Human Services Division, U.S. General Accounting Office; Fritz Streckewald, Associate Commissioner for Program Benefits, the Social Security Administration; Charlotte Twight, professor and privacy expert, Boise State University; and Robert Ellis Smith, editor, the Privacy Journal	27
Paul, Hon. Ron, a Representative in Congress from the State of Texas	12
Letters, statements, etc., submitted for the record by:	
Bovbjerg, Barbara, Associate Director of Education, Workforce, and Income Security Issues, Health, Education, and Human Services Division, U.S. General Accounting Office, prepared statement of	29
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	10
Kleczka, Hon. Jerry, a Representative in Congress from the State of Wisconsin, prepared statement of	25
Paul, Hon. Ron, a Representative in Congress from the State of Texas, prepared statement of	15
Smith, Robert Ellis, editor, the Privacy Journal, prepared statement of	61
Streckewald, Fritz, Associate Commissioner for Program Benefits, the Social Security Administration:	
Information concerning impact of elimination of retirement earnings test	78
Prepared statement of	40
Twight, Charlotte, professor and privacy expert, Boise State University, prepared statement of	52

H.R. 220, THE FREEDOM AND PRIVACY RESTORATION ACT

MAY 18, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Turner.

Staff present: J. Russell George, staff director and chief counsel; Heather Bailey, professional staff member; Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong and Michael Soon, interns; Michelle Ash and Trey Henderson, minority counsels; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

This is the fourth in a series of subcommittee hearings on the issue of privacy. Today, we will examine proposed legislation that would prohibit Federal, State, and local government agencies from using Social Security numbers as identification numbers, except for Social Security and tax purposes. H.R. 220, the Freedom and Privacy Restoration Act of 1999, sponsored by Representative Ron Paul from Texas, in addition to limiting the use of Social Security numbers, the bill would prohibit government agencies from asking individuals for their Social Security number.

The proliferation of personal information on the Internet, in combination with the broad use of the Social Security number, has caused a growing concern over protecting citizens against a rising tide of identity theft associated frauds. When the Social Security number system began in 1936, its purpose was to identify individuals who receive benefits from the Social Security retirement system. Over the years, however, the use of this number has expanded far beyond its original intent. Today, the social number is used as a personal identification number by State and local agencies, utility companies, universities, and a proliferation of private businesses.

Credit bureaus use the number to maintain individual consumer credit histories. State income tax officials use it to identify tax filers. Numerous businesses that sell personal information, offer financial services, and provide health care also rely on the Social Security number. These companies use the number to assess personal

credit ratings, locate assets, maintain health records, and ensure that individuals comply with a variety of rules and regulations.

Clearly, there is a need to protect personal information. There is an equally compelling need to ensure the integrity of Federal programs. Today, the subcommittee will examine whether H.R. 220 is an appropriate balance between those needs.

I will add that we will have a future hearing with individuals that relate to this problem, such as universities across the land, State governments, motor vehicle operations, county registrars. I welcome our witnesses today and look forward to their testimony.

[The text of H.R. 220 and the prepared statement of Hon. Stephen Horn follow:]

I

106TH CONGRESS
1ST SESSION

H. R. 220

To amend title II of the Social Security Act and the Internal Revenue Code of 1986 to protect the integrity and confidentiality of Social Security account numbers issued under such title, to prohibit the establishment in the Federal Government of any uniform national identifying number, and to prohibit Federal agencies from imposing standards for identification of individuals on other agencies or persons.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 6, 1999

Mr. PAUL introduced the following bill; which was referred to the Committee on Ways and Means, and in addition to the Committee on Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend title II of the Social Security Act and the Internal Revenue Code of 1986 to protect the integrity and confidentiality of Social Security account numbers issued under such title, to prohibit the establishment in the Federal Government of any uniform national identifying number, and to prohibit Federal agencies from imposing standards for identification of individuals on other agencies or persons.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the "Freedom and Privacy
3 Restoration Act of 1999".

4 **SEC. 2. RESTRICTIONS ON THE USE OF THE SOCIAL SECU-**
5 **RITY ACCOUNT NUMBER.**

6 (a) REPEAL OF PROVISIONS AUTHORIZING USE OF
7 THE SOCIAL SECURITY ACCOUNT NUMBER.—Subpara-
8 graph (C) of section 205(c)(2) of the Social Security Act
9 (42 U.S.C. 405(c)(2)(C)) is amended by striking "(C)(i)
10 It is the policy" and all that follows through clause (vi)
11 and inserting the following:

12 "(C)(i) Except as otherwise provided in this para-
13 graph, no agency or instrumentality of the Federal Gov-
14 ernment, any State, any political subdivision of a State,
15 or any combination of the foregoing may use a social secu-
16 rity account number issued under this subsection or any
17 derivative of such a number as the means of identifying
18 any individual.

19 "(ii) Clause (i) shall not apply with respect to the
20 use of the social security account number as an identifying
21 number to the extent provided in section 6109(d) of the
22 Internal Revenue Code of 1986 (relating to use of the so-
23 cial security account number for social security and relat-
24 ed purposes).

25 "(iii) If and to the extent that any provision of Fed-
26 eral law enacted before January 1, 2001, is inconsistent

1 with the policy set forth in clause (i), such provision shall,
2 on and after such date, be null, void, and of no effect.".
3 (b) CONFORMING AMENDMENTS.—
4 (1) Clauses (vii) and (viii) of section
5 205(c)(2)(D) of such Act (42 U.S.C.
6 405(c)(2)(D)(vii) and (viii)) are redesignated as
7 clauses (iv) and (v), respectively.
8 (2) Subsection (d) of section 6109 of the Inter-
9 nal Revenue Code of 1986 is amended—
10 (A) in the heading, by inserting "FOR SO-
11 CIAL SECURITY AND RELATED PURPOSES"
12 after "NUMBER"; and
13 (B) by striking "this title" and inserting
14 "section 86, chapter 2, and subtitle C of this
15 title".

16 **SEC. 3. CONFORMING AMENDMENTS TO PRIVACY ACT OF**
17 **1974.**

18 Section 7 of the Privacy Act of 1974 (5 U.S.C. 552a
19 note, 88 Stat. 1909) is amended—
20 (1) in subsection (a), by striking paragraph (2)
21 and inserting the following:
22 "(2) The provisions of paragraph (1) of this sub-
23 section shall not apply with respect to any disclosure which
24 is required under regulations of the Commissioner of So-
25 cial Security pursuant to section 205(c)(2) of the Social

1 Security Act or under regulations of the Secretary of the
2 Treasury pursuant to section 6109(d) of the Internal Rev-
3 enue Code of 1986.";
4 and
5 (2) by striking subsection (b) and inserting the
6 following:
7 "(b) Except with respect to disclosures described in
8 subsection (a)(2), no agency or instrumentality of the
9 Federal Government, a State, a political subdivision of a
10 State, or any combination of the foregoing may request
11 an individual to disclose his social security account num-
12 ber, on either a mandatory or voluntary basis.".

13 **SEC. 4. PROHIBITION OF GOVERNMENT-WIDE UNIFORM**
14 **IDENTIFYING NUMBERS.**

15 (a) IN GENERAL.—Except as authorized under sec-
16 tion 205(c)(2) of the Social Security Act, any two agencies
17 or instrumentalities of the Federal Government may not
18 implement the same identifying number with respect to
19 any individual.
20 (b) IDENTIFYING NUMBERS.—For purposes of this
21 section—
22 (1) the term "identifying number" with respect
23 to an individual means any combination of alpha-nu-
24 meric symbols which serves to identify such individ-
25 ual, and

(2) any identifying number and any one or more derivatives of such number shall be treated as the same identifying number.

SEC. 5. PROHIBITION OF GOVERNMENT-ESTABLISHED IDENTIFIERS.

(a) IN GENERAL.—Subject to subsection (b), a Federal agency may not—

(1) establish or mandate a uniform standard for identification of an individual that is required to be used by any other Federal agency, a State agency, or a private person for any purpose other than the purpose of conducting the authorized activities of the Federal agency establishing or mandating the standard; or

(2) condition receipt of any Federal grant or contract or other Federal funding on the adoption, by a State, a State agency, or a political subdivision of a State, of a uniform standard for identification of an individual.

(b) TRANSACTIONS BETWEEN PRIVATE PERSONS.—Notwithstanding subsection (a), a Federal agency may not establish or mandate a uniform standard for identification of an individual that is required to be used within the agency, or by any other Federal agency, a State agency, or a private person, for the purpose of—

1 (1) investigating, monitoring, overseeing, or
2 otherwise regulating a transaction to which the Fed-
3 eral Government is not a party; or
4 (2) administrative simplification.
5 (c) REPEALER.—Any provision of Federal law en-
6 acted before, on, or after the date of the enactment of
7 this Act that is inconsistent with subsection (a) or (b) is
8 repealed, including sections 1173(b) and 1177(a)(1) of the
9 Social Security Act (42 U.S.C. 1320d–2(b); 42 U.S.C.
10 1320d–6(a)(1)) and section 656 of the Illegal Immigration
11 Reform and Immigrant Responsibility Act of 1996 (5
12 U.S.C. 301 note).
13 (d) DEFINITIONS.—For purposes of this section:
14 (1) AGENCY.—The term "agency" means any
15 of the following:
16 (A) An Executive agency (as defined in
17 section 105 of title 5, United States Code).
18 (B) A military department (as defined in
19 section 102 of such title).
20 (C) An agency in the executive branch of
21 a State government.
22 (D) An agency in the legislative branch of
23 the Government of the United States or a State
24 government.

1 (E) An agency in the judicial branch of the
2 Government of the United States or a State
3 government.
4 (2) STATE.—The term "State" means any of
5 the several States, the District of Columbia, the Vir-
6 gin Islands, the Commonwealth of Puerto Rico,
7 Guam, American Samoa, the Commonwealth of the
8 Northern Mariana Islands, the Republic of the Mar-
9 shall Islands, the Federated States of Micronesia, or
10 the Republic of Palau.

11 **SEC. 6. EFFECTIVE DATE.**

12 The provisions of this Act, including the amendments
13 made thereby, shall take effect January 1, 2001.

○

DAN BURTON, INDIANA
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
T[illegible] S M. DAVIS III, VIRGINIA
[illegible] McINTOSH, INDIANA
[illegible] SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DOOLITTLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Legislative Hearing on H.R. 220, the Freedom and Privacy Restoration Act"

OPENING STATEMENT
REPRESENTATIVE STEPHEN HORN (R-CA)
Chairman, Subcommittee on Government Management, Information, and Technology
May 18, 2000

A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

This is the fourth in a series of subcommittee hearings on the issue of privacy. Today, we will examine proposed legislation that would prohibit Federal, State and local government agencies from using social security numbers as identification numbers, except for social security and tax purposes. H.R. 220, the "Freedom and Privacy Restoration Act of 1999," sponsored by Representative Ron Paul from Texas would also prohibit government agencies from asking individuals for their social security number.

The proliferation of personal information on the Internet in combination with the broad use of the social security number has caused a growing concern over protecting citizens against a rising tide of identity thefts and associated frauds.

When the social security numbering system began in 1936, its purpose was to identify individuals who receive benefits from the social security retirement system. Over the years, however, the use of this number has expanded far beyond its original intent.

Today, the social security number is used as a personal identification number by state and local agencies, utility companies, universities and a proliferation of private businesses.

Credit bureaus use the number to maintain individual consumer credit histories. State income tax officials use it to identify tax filers. Numerous businesses that sell personal information, offer financial services and provide health care also rely on the social security number. These companies use the number to assess personal credit ratings, locate assets, maintain health records, and ensure that individuals comply with a variety of rules and regulations.

Clearly, there is a need to protect personal information. There is an equally compelling need to ensure the integrity of Federal programs. Today, the subcommittee will examine whether H.R. 220 is an appropriate balance between those competing needs.

I welcome our witnesses, and look forward to their testimony.

Mr. HORN. The gentleman from Texas hasn't arrived yet, but we will begin with the other gentleman from Texas.

We have with us the author of the bill, Hon. Ron Paul, a Member of Congress from Texas.

STATEMENT OF HON. RON PAUL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. PAUL. Thank you, Mr. Chairman.

I really appreciate this opportunity and I want to thank you for holding these hearings. The issue of privacy certainly is getting the attention of many people in this country and starting to get the attention of many Members of Congress.

I do have a written statement that I would like to submit.

Mr. HORN. Without objection, your prepared statement will appear in the record.

I might say that the minute we introduce any witness here their full statement goes in automatically.

Mr. PAUL. And I would like to add there is one letter that came from a constituent and I would like to submit that letter as well.

Mr. HORN. Without objection, that letter will also appear in the record.

Mr. PAUL. The issue of privacy certainly has been catching the attention of a lot of people. Last year I introduced this legislation to try to deal with it because we do hear from a lot of our voters who are saying that the Social Security number is being used too often and improperly. In a technical sense, they are right. They are right in the sense that in a free society they are not supposed to be monitored by the Government the way the Social Security number monitors us.

When we established the Social Security number in 1935 or 1936, it was never intended to be a national identifier. In 1970, the Congress passed a bill called the Bank Secrecy Act. That sounds like maybe it would preserve secrecy, but it did exactly the opposite. It made sure the banks knew more about us and the Government got hold of more information.

Congress responded in 1974 by passing the Privacy Act, and it too sounded good and has a very good sentence in there that says the taxpayer and voters will be protected and the Social Security number cannot be used as a national identifier. But unfortunately, in the same piece of legislation, it said that Congress can enact anything they want and mandate the use of the Social Security number.

So Congress since that time has ignored the good statement and picked up on the other statement that said that they do have the authority, according to the Privacy Act of 1974. And Congress has not been bashful. There are 40 different programs now that use the Social Security number as the identifier.

And in 1996, there was a giant leap forward to even expanding this more so because the Immigration Act was written with a mandate for the Transportation Department to develop a national identification card through our drivers' licenses. Fortunately, with some effort, we have been able to rescind that authority.

But also in 1996, the Health Insurance and Portability Act established a need and authority to set up a national data bank and to

have a national medical identifier. And today, with the Government being so involved in medicine, it was argued that this would make it more efficient for Government to monitor and manage medical care because the Government is dealing with the HMOs and this will make it more efficient.

And there is some plausibility to that particular argument, but it also invites the risk, just as happened so often. What looks like a good program always has a down side. The down side is that the Government is going to have all our medical records. And as a physician, I certainly think that is a very dangerous thing because our Government doesn't have a real good record for protecting our privacy. They should be protecting our privacy and there is a lot more time spent invading our privacy.

We do hear stories and they are not limited to one administration where the IRS has been abusive and has been used to invade our privacy. We have also heard about FBI files being abused. So the American people are very, very frightened by all this.

My theory on why we heard so much from our constituents this year on the census wasn't that the census was that more onerous—I think the questions were probably similar to what has been going on for the last 20 or 30 years because they have always asked a lot of questions—but I think the American people now are much more nervous about giving information to the Government. And that is why I think they were complaining so much and worried about it.

And even within the census, they have introduced an idea that they were going to expand on the monitoring approach by having a test in there they actually ask as a test 21,000 people for their Social Security numbers to see what they can learn and how well the people would respond.

So if we don't pay more attention to this, soon the census will be monitored and our numbers will be used to report our numbers and our names to the census. Already today just about everything we do needs a Social Security number. If we're looking for a job, birth certificate, death certificate, bank accounts, medical care—the list goes on and on—drivers' licenses. In most States, you can't even get a fishing license without a Social Security number.

This invites trouble. And one of the worst down sides to this is that by having a universal identification number, it is a good way to bring all our information together of every individual. If we don't do it, we are in trouble with the Government.

And once the information is brought together, the job of identification theft becomes relatively easy. All you have to do is get the Social Security number. And because of Government mandates, we have set it up for them.

My bill deals with this. You can't use your Social Security number for anything other than Social Security. And take away the mandates. Don't tell the States—well, in order for you to get your highway funds, you will put the Social Security number on your drivers' licenses—we wouldn't be able to do that, either.

So this is a broad approach, a serious approach, there is a lot of support for it, but I also understand very clearly the arguments against it because they talk about Government being less effective. They believe they can cut down on fraud if they use the Social Se-

curity number. But the real purpose of Government in a free society is not to make the Government efficient. The purpose of Government in a free society should be to preserve our freedoms.

To me, privacy is equivalent to if not synonymous with freedom. So if we are carelessly willing to sacrifice so much of our privacy and so much of our freedom for the argument that Government may be more efficient, I think is a dangerous direction to be going in.

So this is the reason I bring this to you. I appreciate very much your willingness to listen and look at it because I don't think this issue is going to go away. And I think the nice part about it from my viewpoint—from a civil libertarian viewpoint—is that it isn't a right-wing conservative issue and it is not a left-wing liberal issue. It is a civil libertarian issue which brings in a lot of people from both sides.

And although we get a lot of support and understanding on the need for this, there is also the great hesitation to endorse this because they are frightened about what it might do in handicapping the efficiency of Government.

And I will be glad to yield for questions.

[The prepared statement of Hon. Ron Paul follows:]

RON PAUL
14TH DISTRICT, TEXAS

BANKING AND
FINANCE COMMITTEE

SUBCOMMITTEES:
FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT

DOMESTIC AND INTERNATIONAL
MONETARY POLICY

EDUCATION AND
WORKFORCE COMMITTEE

SUBCOMMITTEES:
WORKFORCE PROTECTIONS

EARLY CHILDHOOD, YOUTH
AND FAMILIES

Congress of the United States
House of Representatives
Washington, DC 20515–4314

Ron Paul

203 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2831

312 SOUTH MAIN
SUITE 228
VICTORIA, TX 77901
(512) 576-1231

301 GUADALUPE
ROOM 105
SAN MARCOS, TX 78666
(512) 396-1400

200 WEST 2ND STREET
SUITE 210
FREEPORT, TX 77541
(409) 230-0600

MOBILE OFFICE
(512) 753-5553

Statement of Ron Paul on the Freedom and Privacy Restoration Act (HR 220)
before the Subcommittee on Government Management, Information and Technology
of the Government Reform and Oversight Committee

05/18/2000

Mr. Chairman, thank you for holding this hearing on my legislation, HR 220, the Freedom and Privacy Restoration Act. I greatly appreciate your commitment to the issue of personal privacy. Protecting privacy is of increasing importance to the American people. Since I have introduced this bill, my office has received countless calls of support from Americans all across the country who are opposed to the use of uniform identifiers. I have also worked with a bipartisan coalition of members on various efforts to protect Americans from the surveillance state, such as the banking regulators' "know your customer" scheme, and the attempt by the Post Office to violate the privacy of all Americans who use Commercial Mail Receiving Agencies (CMRAs).

The Freedom and Privacy Restoration Act represents a comprehensive attempt to protect the privacy of individual citizens from government surveillance via the use of standard identifiers. Among the provisions of the legislation is one repealing those sections of the 1996 Immigration Act that established federal standards for state drivers' licenses and those sections of the Health Insurance Portability and Accountability Act of 1996 that require the Department of Health and Human Services to establish a uniform standard health identifier. As I am sure my colleagues know, the language authorizing a national ID card was repealed in last year's Transportation Appropriations bill and language prohibiting the expenditure of funds to develop a personal medical identifier has been included in the past two Labor-HHS-Education Appropriations bills. These victories where made possible by the thousands of Americans who let their elected representatives know that they were opposed to federally-mandated identifiers.

Perhaps the most significant portion of HR 220 prohibits the use of the Social Security number for purposes not related to Social Security. For all intents and purposes, the Social Security number is already a national identification number. Today, in the majority of states, no American can get a job, open a bank account, get a drivers' license, receive a birth certificate for one's child without presenting their Social Security number. So widespread has the use of the Social Security number become that a member of my staff had to produce a Social Security number in order to get a fishing license!

As a test of citizen resistance, the Census bureau asked 21,000 households to report their Social Security number on their census form. One of the reasons the Census bureau is interested in the

Social Security number is as a key to unlock information held by other government agencies.

Since the creation of the Social Security number in 1935, there have been almost 40 congressionally-authorized uses of the Social Security number as an identification number for non-Social Security programs. Many of these uses, such as the requirement that employers report the Social Security number of new employees to the "new hires data base," have been enacted in the past few years.

Such Congressional actions do not reflect the intent of the Congress that created the Social Security system as that Congress in no way intended to create a national identifier. In fact, Congress never directly authorized the creation of the Social Security number -- they simply authorized the creation of an "appropriate record keeping and identification scheme." The Social Security number was actually the creation of the Internal Revenue Service!

The Social Security number did not become a popular identifier until the 1960s. In response to concerns about the use of the Social Security number, Congress passed the Privacy Act of 1974, because, as stated within the act itself, "The Congress finds the opportunities for an individual to secure employment, insurance and credit and his right to due process and other legal protections are endangered by the misuse of certain information systems."

The Privacy Act of 1974 further states that "It shall be unlawful for any Federal, State or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his Social Security number." This is a good and necessary step toward protecting individual liberty. Unfortunately, the language of the Privacy Act allows Congress to require the use of the Social Security number at will. In fact, just two years after the passage of the Privacy Act, Congress explicitly allowed state governments to use the Social Security number as an identifier for tax collection, motor vehicle registration and drivers' license identification. When one considers the trend toward the use of the Social Security number as an identifier, the need for HR 220 becomes clear.

The Freedom and Privacy Restoration Act also contains a blanket prohibition on the use of identifiers to "investigate, monitor, oversee, or otherwise regulate" American citizens. Mr. Chairman, prohibiting the Federal Government from using standard identifiers will ensure that American liberty is protected from the "surveillance state." Allowing the federal government to use standard identifiers to oversee private transactions present tremendous potential for abuse of civil liberties by unscrupulous government officials.

I am sure I need not remind the members of this Committee of the sad history of government officials of both parties using personal information contained in IRS or FBI files against their political enemies. Imagine the potential for abuse if an unscrupulous government official is able to access one's complete medical, credit, and employment history by simply typing the citizens' "uniform identifier" into a database.

This history of abuse of personal information by government officials demonstrates that the only effective means of guaranteeing American's privacy is to limit the ability of the government to

collect and store information regarding a citizen's personal matters. The only way to prevent the government from knowing this information is to prevent them from using standard identifiers.

In addition to forbidding the federal government from creating national identifiers, this legislation forbids the federal government from blackmailing states into adopting uniform standard identifiers by withholding federal funds. One of the most onerous practices of Congress is the use of federal funds illegitimately taken from the American people to bribe states into obeying federal dictates.

Certain members of Congress are focusing on the use of the Social Security number and other identifiers by private businesses. However, this ignores the fact that the private sector was only following the lead of the federal government in using the Social Security number as an ID. In many cases, the use of the Social Security number by private business is directly mandated by the government, for example, banks use Social Security numbers as an identifier for their customers because the federal government required them to use the Social Security number for tax reporting purposes. Once the federal government stops using the Social Security number as an identifier, the majority of private businesses, whose livelihood depends on pleasing consumers, will respond to their customers demands and stop using the Social Security number and other standard identifiers in dealing with them.

I hope that we in Congress would not once again allow a problem Congress created to become an excuse for disregarding the constitutional limitations of federal police powers or imposing new mandates on businesses in the name of "protecting privacy." Federal mandates on private businesses may harm consumers by preventing business from offering improved services such as the ability to bring new products that consumers would be interested in immediately to the consumers' attention. These mandates will also further interfere with matters which should be resolved by private contracts.

Furthermore, as we have seen with the administration's so-called "medical privacy protection" proposal, federal "privacy protection laws" can actually undermine privacy by granting certain state-favored interests access to one's personal information.

Some my claim that the federal government needs expanded surveillance powers to protect against fraud or some other criminal activities. However, monitoring the transactions of every American in order to catch those few who are involved in some sort of illegal activity turns one of the great bulwarks of our liberty, the presumption of innocence, on its head. The federal government has no right to treat all Americans as criminals by spying on their relationship with their doctors, employers, or bankers. In fact, criminal law enforcement is reserved to the state and local governments by the Constitution's tenth amendment.

Others may claim that the federal government needs the power to monitor Americans in order to allow the government to operate more efficiently. However, in a constitutional republic the people are never asked to sacrifice their liberties to make the job of government officials a little bit easier. We are here to protect the freedom of the American people, not to make privacy invasion more efficient.

The main reason Congress should take action to stop the use of standard identifiers is because the federal government lacks constitutional authority to force citizens to adopt a universal identifier for health care, employment, or any other reason. Any federal action that oversteps constitutional limitations violates liberty because it ratifies the principle that the federal government, not the Constitution, is the ultimate judge of its own jurisdiction over the people. The only effective protection of the rights of citizens is for Congress to follow Thomas Jefferson's advice and "bind (the federal government) down with the chains of the Constitution."

I once again extend my sincere appreciation to Chairman Horn and the other members of the Subcommittee for holding this hearing and express my hope that this hearing begins the process of protecting the rights of all citizens to conduct their lives free from government intrusion.

Mr. HORN. Let me ask you about Medicare.

When we drafted the Medicare bill—and I was on that team in the Senate staff in 1965—we followed essentially how Social Security had done it and we modelled the Medicare part on it.

Now, would you permit the use of the Social Security number for medical files in Medicare, since it is needed to make sure there are real people getting benefits and not somebody that has a number—and there is no question there is a lot of misuse of the number in terms of people looking at the dead and all the rest. If it hasn't been changed in Baltimore, I guess they get away with it. But we will get some testimony on that later.

But how do you feel about including Medicare with a Social Security number.

Mr. PAUL. My first thoughts are psychologically, in my mind, without thinking it through in detail legally—I think of Medicare and Social Security being pretty close together. I think if that were the only problem, I don't think I would be here with this piece of legislation. But I think if we were to use it for Medicare, it could be very, very strictly limited to that with the idea that that is part of the Social Security system, because I think of it as the same. I think of it as the same.

But I think when you get into the other medical programs, whether it is the managed care system the Government has so much to do with or the Medicaid system and on and on, then I would not be nearly that generous. I would say that you should have another identifier because there will always be the efficiency argument, whether it is an educational program or a medical program. But strictly limited to Medicare for the protection of the individuals I think is very important.

Mr. HORN. In the testimony we expect to hear on the next panel, it will be pointed out that if there isn't a common identifier when Government agencies attempt to locate that it creates a problem. For example, dead-beat dads, people with similar names may be mistakenly identified and there is a real problem where the people aren't submitting their alimony ordered by the court, they move across county lines in California or they move across State lines.

How would you address that problem if your bill became law?

Mr. PAUL. I think States faced this problem prior to the time we had Social Security because I don't think of dead-beat dads as a separate issue. I think that is a problem of someone not paying their bills and meeting up to their financial responsibilities. So I would say that is a State issue. And if you are dealing with a cross-State problem, then those two States have to get together and work it out.

But prior to even the 1960's, we didn't have that because it was only in the 1960's when we started really using it. And even in the 1970's when we dealt with all the financial accounts—we didn't even have the Social Security numbers on our tax returns until 1961.

So I would say that that is not the job of the Federal Government or the Congress to facilitate this collection. This is a very serious problem, but prior to the Social Security number, it was handled as adequately as it is today, I am sure.

Mr. HORN. Well, I remember one study we had a few years ago on Pell grants. Those are the ones that generally help the State schools and colleges. One person was eligible on Pell grants in terms of the information he showed at the student financial aid office, but actually he was a millionaire, and that was found through interconnection of his Social Security number with that in the tax record.

Does that bother you?

Mr. PAUL. It bothers me that fraud was committed, but I do not think that we eliminate the prosecution of fraud by preserving freedom for the large majority of people. We shouldn't sacrifice the privacy of 99 people because you might catch one person that is going to commit fraud. I don't think we sacrifice our ability to pursue fraud because there would be ways of finding out if this person lied. But at the same time, you don't want to penalize and assume somebody is guilty of something and put a tremendous burden on them to follow so many of these privacy laws and let the Government accumulate this information.

I think the supposed benefit is not worth the sacrifice of personal liberty.

Mr. HORN. My last question, and then I'll turn it over to my colleague, Mr. Turner, your colleague from Texas.

The written testimony of some of the second panel witnesses suggests adding a penalty section.

What is your view of that idea?

Mr. PAUL. A penalty?

Mr. HORN. If you misuse the Social Security number, should there be a penalty?

Mr. PAUL. I certainly think there should be a penalty on the U.S. Government when they misuse the Social Security number. But we should just prohibit by law the abuse of the Social Security number and then there would be—I think they use it because they have been granted the authority to use it and we encourage it. As we set up a new program, we are always anxious. The Social Security number is great. So we literally have it from cradle to grave now.

Are you thinking about a businessman misusing the Social Security number?

Mr. HORN. Your bill, if it was put on the law books, do you think there ought to be a penalty section to make sure that the people obey that particular bill?

Mr. PAUL. And you are referring to Government people?

Mr. HORN. I am referring to anybody who uses the Social Security number, because I am assuming that is what you are banning in your bill.

Mr. PAUL. I hadn't thought about that, and maybe I am overly optimistic that if we pass a law and say "Thou shalt not use the Social Security number," I would expect that we wouldn't use the Social Security number. I would think that if it were abused and the Social Security number was being forced on a State or Congress kept passing these laws, I guess the only penalty would be eventually at the polls. The American people would have to invoke the penalty.

Right now, I think we are getting close to that point where the American people are getting nervous about the invasion of their

privacy and it is an issue that they would like to hear more about from us.

Mr. HORN. So you don't feel that a penalty section is needed?

Mr. PAUL. Well, at the moment, I don't. But I would have to admit I haven't thought it through completely and I would certainly be open to suggestions on that, if I could see the need for it.

Mr. HORN. Well, I thank you and I now yield to the gentleman from Texas, the ranking member here, Mr. Turner for an opening statement as well as questioning the witness.

Mr. TURNER. Thank you, Mr. Chairman.

Welcome, Mr. Paul, a fellow Texan. It is always good to have Texans before our committee.

There is another bill that Mr. Kleczka has that would ban the use of the Social Security number in both the public and private sector. I know you addressed that in your opening remarks, but expand on that a little bit. Why, if you fear the use of the Social Security number by Government agencies contributes to the invasion of our privacy, why wouldn't you just tell the private sector they shouldn't use it as well?

Mr. PAUL. Well, I deal with that but a little more indirectly because if the private sector uses that number mainly because we have made it convenient for them to use it and we have mandated it too often when it comes to financial records—I mean, we tell the banks what to do—and anytime we do anything we put the pressure on them to use that number. Then they accumulate the information and they are tempted to sell it and do whatever.

I think the fact that we do get them to accumulate all this information makes it much easier for identity theft. But I don't think the answer to our problem is dealing with another set of regulations on business people. Like last year when we passed the banking legislation, we said that what we needed to do was make sure that some of this information isn't transferred within a certain corporation or closely in-line corporation. But what that actually did was mandated more forms to be filled out, which means there is more information accumulated under the Social Security number.

I think the abuse in the private sector comes as a secondary consequence. If we weren't using it so much, there would be no reason for them to do it. But I don't see the answer coming by just putting another constraint or another form to be filled out by the private sector. I don't see that's where the problem is.

Mr. TURNER. So you think the private sector would just slowly quit using the Social Security number? There are obviously multitudes of records that have all of us identified by our Social Security number.

Mr. PAUL. If we didn't tie it all together, I think they would lose their enthusiasm for using it. I don't see a convenient way of saying—we could say it, but could you imagine telling every individual that they are not allowed to use it? That means that we would have more snooping to make sure that nobody ever asked somebody for their Social Security number.

But I think the abuse in this area should be dealt with on a property rights issue, fraud issue, local issue, but not by leaving the system in place and coming up with more of a rule. And this

is our temptation here, instead of looking at the basic problem, we are more tempted to come in and set up more rules and regulations on the private sector and not dealing with the source of the problem, which was our carelessness in allowing the universal identifier to be developed.

Although it is not admitted that it is here and we have had a couple of victories like "Know Your Customer"—that is something I don't think too many of us supported and they withdrew it. That was more banking regulations. As well, there was the National I.D. Card Authority. We got that removed.

So we have minor victories, but I don't think overall we have reversed the trend. The need for, the desire for, and the so-called benefits of a universal identifier are very, very strong. I think that is where the problem is and not with the private sector participating in the use of a Social Security number when they probably don't even need to.

Sometimes you wonder why so many businesses are always asking you for these Social Security numbers, even when it's not the law. But people have been so conditioned to do it. So we have the Government mandating the encouragement, everybody accepts the Social Security number, and then we have businesses sort of jumping on.

So I think the solution is back to making sure that we do not establish the principle of a national identifier. That is what my bill deals with.

Mr. TURNER. Have you been able to address the cost of the abandonment of the use of the Social Security number by the Federal Government agencies?

Mr. PAUL. No, not directly. But I know the cost of not doing it is very, very high in terms of privacy and individual liberty, and that is the cost I am looking at because there is such an intrusion as a cost-in that we facilitate identification theft—so that cost is tremendous. How much the cost would be if we continue with our same type of Federal education programs and medical programs—if they had different numbers, I am not sure there would be a tremendous increase in cost on that. They would just have to come up with a different number.

Mr. TURNER. I guess there would also be some cost to State governments, maybe even local governments that have come to rely on the Social Security number.

Mr. PAUL. They would have to quit relying on it.

In the State of Texas, you know that it is only recent that we have had to give our Social Security number. It isn't on our driver's license, but that is the direction that we were and probably still are moving in, that every State will have a universal driver's license with Social Security numbers. But we are now required to give it even though it doesn't appear. So there is the connection. The intertwining of being able to monitor and know everything about everybody is the universal identifier, which is the Social Security number.

I don't want any pressure—in fact, my bill deals with this. We as a Congress cannot put pressure on the State to use the Social Security number. Maybe your question is saying that the State

wants to. I think if we take away the incentive, the pressure, and the mandates, they are less likely to.

Mr. TURNER. We had a hearing just the other day in this committee on a proposal by Representative Hutchinson to have a study commission on the issue of privacy. I know we have several bills that are moving through the Congress, some regulations that have been proposed trying to protect our privacy.

Do you feel that we can point to some specific abuses that relate to the use of the Social Security number where our privacy has been invaded? Do we have some specific examples on a wider scale that might point out the scope of the problem that you perceive to exist?

Mr. PAUL. I don't think that would be difficult to find. Certainly the notion that we have a medical data bank, and assuming that there would never be a violation is almost too much to believe. And we do know specifically that our Government too often has abused records like FBI records and IRS records and they were never to be used in the political sense. Yet I think both administrations have been guilty of abuse in using these records in a political sense.

I think people really are fearful of the Government having their medical records. And we make no in-roads at all—we have made in-roads on the National I.D. Card, but we have made no progress at all in slowing up the National Medical Data Bank with the Social Security number as the identifier.

I can't show you an example of how the Government has abused that, but gut instinct tells us it is not a very good idea and the American people don't want it. That I am sure of.

Mr. TURNER. Of course, the medical records are by and large in the private sector. Would there perhaps be some way to center in on specific areas that are particularly sensitive, like medical records and perhaps do something in that area rather than just across the board?

Mr. PAUL. But that really confuses the movement toward the universal health care because we are moving in that direction because so much is managed health care and HMOs. Once Medicare starts paying for HMOs, they have to monitor it and they have to make sure that patients don't abuse it, doctors don't abuse it, hospitals don't abuse it. There is always the temptation to abuse the system, so the argument will be that we have to be able to monitor it.

They use the idea that we need this information because it is good to study health. We get statistics and we can learn more about medicine. There will be all these wonderful things that they are going to do. So the odds of us developing a medical care system that is being developed and be able to maintain medical records, as I did for 30 years—my medical records were in the office in a filing cabinet and that was it. But now, when you get into the managed care system and the HMO, they can march in and look at your medical records and find out whether you have been abusing medical care. They will just go through your file.

For efficiency sake, they want these files changed. If somebody moves to New York, they don't want it the old-fashioned way where you mail the records or the patient carries them, they want HHS

to have access to this and just transfer these medical files. That is what is coming unless we are able to stop this.

Even my bill doesn't deal with that overall problem as much as it slows it up in that it wouldn't have the universal identifier. I would like to address the medical care system in this country, but that is not what this does. It just says that if you are going to move in the direction of a single payer, universal health care system in this country—which we are moving rapidly toward—that they cannot use the Social Security number so that they can do the matching up.

When people want to know about individuals and they have a Social Security number, they can look up and find every piece of property owned, what your bank account is, and what kind of disease you have, it will undermine the practice of medicine like you have never seen it. I have talked to other physicians and the natural tendency is to not keep good medical records.

If somebody comes in and has controversial things to talk about, the good doctor is not going to write it down because it is not going to be private. We are moving in that direction. And the other physicians in Congress have admitted that to me already, that they have the same concerns.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. I just have one comment on this, and that is numberitis. There is a very interesting editorial in the Newark, NJ Star Ledger. The columnist and editorial board notes: "We are challenged to remember e-mail addresses, office extension numbers, fax numbers, paging I.D.'s, PIN numbers, Web site addresses. The other day I telephoned a greenhouse manufacturer to buy some supplies. The service representative wanted to know my customer identification number. I told the woman I hadn't a clue. Then she asked for a serial number, but I wasn't about to trot out to the greenhouse and copy it down. Finally, she settled for my zip code and, bingo, I was able to place my order. We must be given the third degree every time we want to purchase something. Do we really have to?"

Then it goes on, "In simpler times, all I had to know was my Social Security number and a couple of phone numbers. Now my head is so loaded with codes and personal identification numbers that it is understandable why my memory bank crashes from time to time. I am not a techie or a geek. Programming isn't my strong suit. I have given up, for instance, the notions that I will ever learn how to program a video recorder. Besides, I have neither the time nor the inclination to sit down and program numerical codes into, say, a palm pilot."

So there are a lot of aspects of this and we appreciate you coming here. Since my colleague, Mr. Turner, mentioned Representative Kleczka's statement here, if you would like it put in the record here at this point——

Mr. TURNER. Yes, Mr. Chairman, Mr. Kleczka requested that we include his statement in the record.

Mr. HORN. Without objection, his prepared statement will appear in the record.

[The prepared statement of Hon. Jerry Kleczka follows:]

Statement of Rep. Jerry Kleczka before the Government Reform Subcommittee on Government Management and Technology
Thursday, May 18, 2000

Mr. Chairman and Ranking Member Turner, thank you for permitting me to express my views to the Subcommittee regarding Rep. Paul's legislation, H.R. 220, to restrict the government use of Social Security numbers. As you know, I recently testified on a panel with Dr. Paul before the Ways and Means Social Security Subcommittee on the use and misuses of Social Security numbers (SSNs).

I agree that the Social Security number has become a de facto national identification number. In fact, last year, myself and Dr. Paul worked together to give Members of the next Congress the option to not include their SSN on their voting cards.

The motives behind H.R. 220 are noble, but more needs to be done. I have introduced legislation, H.R. 1450--the Personal Information Privacy Act (PIPA), that will restrict the private sector uses of the Social Security number by allowing only those uses explicitly authorized in current law.

H.R. 1450 would allow credit headers to include only names and addresses. The credit header could include an individual's telephone number only if it is already listed in the phone book. Currently, information such as Social Security numbers and mothers' maiden names are available on credit headers, which are not protected by the Fair Credit Reporting Act (FCRA). Under the FCRA, a person can purchase a credit report only if they are making a firm offer of credit or insurance; or if they have the consumer's consent. Credit headers, which contain the aforementioned sensitive information, have no such protections and may be purchased by anyone.

In addition, PIPA would prohibit the purchase and or sale of Social Security numbers without the owner's written consent. This legislation would also prohibit the use of an individual's SSN for identification purposes without the written consent of the individual. In order for consent to be valid, the person desiring to use an individual's SSN must inform the individual of all the purposes for which the SSN will be utilized, the persons to whom the number will be known, and obtain the individual's consent in writing. These protections are similar to those contained in the Privacy Act of 1974, which restricts the federal government's uses of SSNs.

While Rep. Paul's bill raises awareness of the many government uses of the SSN that are not related to the Social Security program, the types of privacy protections that the federal government has for the use of SSNs should also be applied to the private sector.

Mr. HORN. It is rather interesting. He has a bill in also and his bill is H.R. 1450, which is the Personal Information Privacy Act [PIPA]—we are getting just like the executive bureaucracy here.

He said H.R. 1450 would allow credit headers to include only names and addresses. The credit headers could include an individual's telephone number only if it is already listed in the phone book. Currently, information such as Social Security numbers and mother's maiden names are available on credit headers, which are not protected by the Fair Credit Reporting Act. Under the FCRA, a person can purchase a credit report only if they are making a firm offer of credit or insurance or if they have the consumer's consent. Credit headers, which contain the aforementioned sensitive information have no such protections and may be purchased by anyone.

It is a very interesting bill, also. Have you had a chance to look at that?

Mr. PAUL. Not in great detail, but we have talked about it and we testified in another committee on that. Jerry and I have worked closely together because we have written a letter to the clerk about why our Social Security numbers are on our voting cards. So we can't even vote without Social Security number, but most of us have not paid much attention to it.

They claim that they give us a chance to have it on or not, which isn't exactly true. So maybe next go around everybody is going to have to fill out a form on whether we want our Social Security number on our voting card or not. Maybe if we don't have a Social Security number we won't get to vote.

Mr. HORN. And they will probably ask us to put the Social Security number on the form we fill out, right?

Mr. PAUL. That's right.

Mr. HORN. Thank you so much for coming. You are going to stimulate quite a discussion nationwide on this, I think. But I think it is a worthwhile endeavor.

We will now go then to panel two. If Barbara Bovbjerg, Hon. Fritz Streckewald, Charlotte Twight, and Robert Smith will come forward, we will swear you in. If you have staff behind you that will be possibly testifying, please have them stand up and the clerk will take their names and we will have them affirm the oath.

[Witnesses sworn.]

Mr. HORN. We have six people. The clerk will get the names of those behind Dr. Twight.

We will start down the line with Ms. Bovbjerg, Associate Director of Education, Workforce, and Income Security Issues for the Health, Education, and Human Services Division of the U.S. General Accounting Office, which is part of the legislative branch and does a wonderful job in terms of both programmatic analysis and fiscal analysis. We are glad to see you.

STATEMENTS OF BARBARA BOVBJERG, ASSOCIATE DIRECTOR OF EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES, HEALTH, EDUCATION, AND HUMAN SERVICES DIVISION, U.S. GENERAL ACCOUNTING OFFICE; FRITZ STRECKEWALD, ASSOCIATE COMMISSIONER FOR PROGRAM BENEFITS, THE SOCIAL SECURITY ADMINISTRATION; CHARLOTTE TWIGHT, PROFESSOR AND PRIVACY EXPERT, BOISE STATE UNIVERSITY; AND ROBERT ELLIS SMITH, EDITOR, THE PRIVACY JOURNAL

Ms. BOVBJERG. Thank you. I am happy to be here.

Mr. Chairman and members of the subcommittee, I am really pleased to be here today to discuss uses of the Social Security number.

Mr. HORN. I should say one more thing.

We all have the written statement. We would like you to summarize it in 5 minutes. If you need 10, we will get to that, but go ahead.

Ms. BOVBJERG. I will make it in 5 minutes.

Almost 277 million Americans have been assigned a SSN, and because each is unique to the individual, the SSN is frequently used for a variety of purposes. Privacy concerns, coupled with mounting instances of identity theft have raised public sensitivity to this issue.

I would like to focus my remarks on three aspects of the topic: the Federal role in the use of the SSN, State and private sector use, and finally the possible impact of restricting the number's use. My testimony is based on a report we prepared in 1998.

First, the Federal role.

No single Federal law regulates the overall use of the SSN, but several require its use to help enforce the law, determine benefit eligibility, or both. For example, the Internal Revenue Code requires that the SSN serve as the taxpayer identification number. This means that taxpayers must report their SSN when they pay taxes, and their SSNs must also be known to their employers and financial institutions from whom they receive income.

Federal law also requires individuals to provide their SSN when they apply for means-tested benefits such as supplemental security income, Medicaid, food stamps. The numbers are used not only for recordkeeping but also to verify income that individuals report.

For example, the Social Security Administration matches records with other entities such as the Department of Veterans' Affairs to identify SSI applicants who may also be receiving other benefits, and does so by using the SSN as the unique identifier. Federal law also requires States to use SSNs in their child support enforcement programs, in issuing commercial drivers' licenses, and on a variety of documents such as marriage licenses and death certificates.

Federal law generally does not restrict SSN use, except in a few instances. The Privacy Act of 1974 restricts Federal agencies in collecting and disclosing personal information, such as SSNs without the individual's consent. The Driver's Protection Policy Act restricts State governments from disseminating the SSN with drivers' license databases.

I would like to turn now to how SSNs are used outside the Federal Government.

In our work, we focused on those users who reach the largest number of people: State governments and, for the private sector, businesses that offer health services, financial services, or personal information.

State officials say they use SSNs in both administering programs and in enforcing the law. For example, State tax administrators routinely use the SSN as a primary identifier in their tax systems and to cross-check taxpayer income. State driver licensing agencies most typically use SSNs to check an individual's driving record in other States. Law enforcement agencies use SSNs to check criminal records.

In the private sector, the health care industry generally uses SSNs as back-up identifiers. Other numbers serve as primary identifiers for patient medical records. But SSNs are needed to trace patients' medical care across providers or to integrate patient records when providers merge.

Credit bureaus also use SSNs. Such organizations build databases of consumer payments and credit transactions. Credit bureaus use the SSN as a principal identifier for retrieving credit histories on demand. Most of their customers—insurance companies, collection agencies, credit grantors—provide a SSN when requesting a credit history and can deny credit to individuals who refuse to provide them.

In contrast to these administrative uses, businesses that sell personal information collect SSNs for the sole purpose of selling them in a linkage with other information. Generally, these databases use SSNs to facilitate records searches when they are sold to customers like debt collectors, employers, anyone who may want to carry out some form of background check on an individual.

Finally, I would like to summarize the possible effects of restricting use of the SSN. Users told us that without the SSN as a unique identifier, data exchanges would be at risk. Tax enforcement would be hampered by not being able to verify income reported. Stewardship of public benefit programs would weaken. States could not readily identify drivers concealing out-of-State traffic violations. Consumer credit histories could not be quickly updated and accurately retrieved.

In conclusion, wide use of the SSN is permissible, but its presence in databases creates privacy concerns and fosters the growing problem of identity theft. In considering restrictions on the use of the SSN, these privacy and confidentiality concerns must be weighed against the Government's need for timely and accurate information to prevent fraud and abuse and against the public preference for services, like easy credit, that are enhanced by the use of the SSN.

Mr. Chairman, that concludes my statement. I am available for questions.

[The prepared statement of Ms. Bovbjerg follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m.
Thursday, May 18, 2000

SOCIAL SECURITY

Government and Other Uses of the Social Security Number are Widespread

Statement of Barbara D. Bovbjerg, Associate Director
Education, Workforce, and Income Security Issues
Health, Education, and Human Services Division

GAO/T-HEHS-00-120

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to discuss usage of the Social Security number (SSN). The SSN was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. Today over 277 million individuals have a unique SSN. For this reason it is used for myriad purposes not related to Social Security. Both private businesses and government agencies frequently ask individuals for their SSNs because in certain instances they are required to or because SSNs provide a convenient means to track and exchange information.

Perceived widespread sharing of personal information and occurrences of identity theft have raised public concern. To provide information about how the SSN is currently used, in my remarks today I will describe (1) the ways that the federal government uses SSNs and current restrictions on these uses, (2) the nonfederal purposes for which the number is used, and (3) what businesses and state governments believe the effect would be if federal laws limiting the use of SSNs were passed. My testimony is based on findings from a study[1] we conducted during 1998 and recent work conducted to update our information.

In summary, the federal government, state and local governments, and private businesses all widely use SSNs. In the case of the federal government, a number of laws and regulations require the use of SSNs for various programs, but they generally also impose limitations on how these SSNs may be used. However, no federal law imposes broad restrictions on businesses' and state and local governments' use of SSNs when that use is unrelated to a specific federal requirement. Currently, governments and businesses frequently use SSNs to identify and organize individuals' records. Some may also use SSNs to exchange information with other organizations to verify information on file, to coordinate benefits or services, or to ensure compliance with certain federal laws. For example, by sharing information about applicants for the Supplemental Security Income (SSI) program, the Social Security Administration (SSA) can identify individuals whose benefits should be reduced, such as those in prison. In addition, some information brokers use SSNs to retrieve the large amount of personal information on individuals that they collect and sell. Public concern over the availability of personal information has encouraged some to consider ways to limit using SSNs to disclose such information. However, officials from both state governments and private businesses have stated that if the federal government passed laws that limited their use of SSNs, their ability to reliably identify individuals' records would be limited, as would their subsequent ability to administer programs and conduct data exchanges with others. Nonetheless, some state agencies and businesses have voluntarily taken steps to limit their disclosure of SSNs.

[1] *Social Security: Government and Commercial Use of the Social Security Number Is Widespread* (GAO/HEHS-99-28, Feb. 16, 1999).

FEDERAL LAWS AND REGULATIONS REQUIRE AND RESTRICT CERTAIN SSN USES

Although SSA originally intended SSNs as a means to identify workers' earnings and eligibility for Social Security benefits, a number of federal laws and regulations now require the use of the SSN to track participation in a variety of federal programs. Use of SSNs facilitates automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both.

The Internal Revenue Code and regulations that govern the administration of the federal personal income tax program require that individuals' SSNs serve as taxpayer identification numbers. Employers and others making payments to individuals must include the individual's SSN in reporting to the Internal Revenue Service (IRS) many of these payments. Reportable payments include interest payments to customers, wages paid to employees, dividends paid to stockholders, and retirement benefits paid to individuals. Other reportable transactions include purchases involving more than $10,000 cash and mortgage interest payments totaling $600 or more. In addition, the Code and regulations require that individuals filing personal income tax returns include their SSN and those of any dependents or former spouses to whom they pay alimony. Using the SSNs, the IRS matches the information supplied by entities reporting payments or other transactions with returns filed by taxpayers to monitor individuals' compliance with federal income tax laws.

Similarly, the Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, food stamp, Temporary Assistance for Needy Families (TANF), and Medicaid programs—programs that provide benefits to people with limited income. Applicants give program administrators information about their income and resources, and program administrators use applicants' SSNs to match records with those of other organizations to verify the information. Using SSNs to match records enhances program payment controls and reduces fraud and abuse. For example, SSA uses SSNs to determine whether applicants for SSI benefits have accurately reported their income by matching records with the Department of Veterans Affairs, the Office of Personnel Management, and the Railroad Retirement Board to identify any retirement or disability payments to these individuals. In fact, we have recommended in previous reports that SSA match its records with other state and federal program records to reduce SSI payments to individuals whom agencies find residing in nursing homes and prisons. In 1997, SSA estimated that overpayments to individuals in nursing homes may have exceeded $100 million annually because SSA was unaware that some SSI benefit recipients were in facilities where their care was paid by Medicaid, and thus they continued to receive SSI benefits.[2] In recent years, SSA has made approximately $1 billion in annual overpayments to SSI recipients. It is especially important to prevent these overpayments because recovering them once they have been paid out is difficult. The gap between what is collected and what is owed the SSI program is continuing to grow each year.

[2]In August 1999, SSA began conducting monthly computer matches with nursing home admissions data obtained from all states.

Similarly, the Commercial Motor Vehicle Safety Act of 1986 requires states to use individuals' SSNs to determine if an individual holds a commercial license issued by another state. This checking is necessary because commercial drivers are limited to owning one state-issued driver's license. States may also use SSNs to search a database to determine whether an applicant's license has been cancelled, suspended, or revoked by another state. In these situations, states use SSNs to limit the possibility of inappropriately licensing applicants. Also, federal law requires that states use SSNs to maintain records of individuals who owe state-ordered child support or are owed child support and to collect from employers reports of new hires identified by SSN. States then transmit this information to the Federal Parent Locator Service, an automated database searchable by SSNs. The use of SSNs in these instances ensures compliance with federal tax laws, enhances program payment controls, reduces the possibility of inappropriately licensing applicants, and facilitates enforcement of child support payments.

Federal laws that require the use of an SSN generally limit its use to the statutory purposes described in each of the laws. For example, the Internal Revenue Code, which requires the use of SSNs for tax purposes, also declares tax return information, including SSNs, to be confidential and prescribes both civil and criminal penalties for unauthorized disclosure. Similarly, the Social Security Act, which requires the use of SSNs for disbursement of benefits, declares that SSNs obtained or maintained by authorized individuals on or after October 1, 1990, are confidential and prohibits their disclosure. Finally, the Personal Responsibility and Work Opportunity Act, which expanded the Federal Parent Locator Service, explicitly restricts the use of SSNs to purposes set out in the act, such as locating absentee parents to enforce child support payments.

In addition to the restrictions contained in laws that require the use of SSNs, the Privacy Act of 1974 also restricts federal agencies in collecting and disclosing personal information, which includes SSNs. The act requires federal agencies that collect information from individuals to inform the individuals of the agencies' authority for requesting the information, whether providing the information is optional or mandatory, and how the agencies plan to use the information. The act, which also prohibits federal agencies from disclosing information without individuals' consent, does not apply to other levels of government or to private businesses.

Except as discussed above, federal law does not regulate the use of SSNs. Thus, nonfederal agencies and legitimate businesses use SSNs in ways not covered by federal law, which I will now discuss.

GOVERNMENTS AND BUSINESSES USE SSNs EXTENSIVELY

Because there are so many users of the SSN, I will focus on organizations that routinely use SSNs for activities that affect a large number of people. These include state government agencies as well as private businesses that sell health services, financial services, and personal information. In general, organizations may record SSNs in their databases for two purposes: to locate records for routine internal activities, such as maintaining and updating account information and, more frequently, to facilitate information exchanges with other organizations.

Governments, health care organizations, and financial services businesses use SSNs, at least in part, to perform services for the person who owns the number. Information brokers, however, collect information that may include SSNs for the sole purpose of selling it.

State Agencies

States use SSNs to support state government operations and offer services to residents. The Social Security Act allows states to use SSNs to identify individuals who pay taxes, receive general public assistance, own a vehicle, or drive. My comments today will focus on two examples of how states use SSNs to administer programs: states' personal income tax programs and licensing of drivers.

All states that have personal income tax use SSNs to administer their programs, according to an official at an organization representing state tax administrators. States use SSNs as primary identifiers in their programs and for auditing purposes. Tax administrators from Maryland and Virginia told us that their states require individuals to provide their SSNs on state tax returns and that those who do not risk being considered nonfilers if tax administrators cannot otherwise identify them. In order to monitor taxpayer income reporting, states rely on SSNs to match data with IRS and state tax agencies. In addition, tax administrators said they use SSNs to cross-reference owners' or officers' business income tax returns with their personal income tax returns so that an audit of one triggers an audit of the other. They also use SSNs to identify residents who received income or tax credits in other states. Finally, when they assess liens against a taxpayer, tax administrators may also use SSNs to gather information from credit bureaus and information brokers about a taxpayer's assets.

State driver licensing agencies are more likely to use SSNs to exchange data with other organizations than to support internal activities. Information from the American Association of Motor Vehicle Administration (AAMVA) and other sources suggests that many states request, but may not require, applicants for noncommercial driver licenses to provide their SSNs. Most state driver licensing agencies that request SSNs include SSNs in driver records as a secondary identifier and devise their own license numbers. To monitor drivers' compliance with state laws, state officials said they use SSNs during the licensing process to search national databases maintained by AAMVA. This allows states to identify driver licenses an applicant may hold in other states and to determine whether the applicant has had a license suspended or revoked in another state. Licensing officials told us that courts and law enforcement agencies may request driver records by SSN when they do not know the driver's license number. In the past, some states have sold personal information collected from drivers and automobile owners, including SSNs, to individuals and businesses. However, the federal Drivers' Privacy Protection Act now prohibits states from disclosing this personal information for purposes such as surveys, marketing, and solicitation without the express consent of the individual.[3]

[3]Until a 1999 amendment to the act, states were permitted to disclose this information if they provided drivers with the opportunity to prohibit disclosure and the driver opted not to do so.

Having discussed how state governments use SSNs, I would like now to focus on how private businesses use these numbers. Specifically, I will discuss use of SSNs by health care service organizations, financial services businesses, and businesses that sell information.

Health Care Services Organizations

Officials representing hospitals, a health maintenance organization (HMO), and a health insurance trade association told us that their organizations always ask for an SSN, but they do not deny services if a patient refuses to provide the number.

Officials from a hospital and an HMO told us that although they ask patients for their SSNs, they assign patients other identifying numbers, which they use internally as the primary identifiers for patient medical records. If a patient either forgets or does not know the patient number he or she was assigned then the hospital or HMO uses SSNs as a backup to identify records. These officials also told us that hospitals and HMOs use SSNs to track patients' medical care across multiple providers because doing so helps establish a patient's medical history and avoid duplicate tests. Similarly, health care providers use SSNs to integrate patients' records when providers merge, a trend that is growing.

We also spoke with a representative from a health insurance trade association to understand how insurers use SSNs. He told us that some health insurers use the SSN or a variation of the number as the customer's insurance number. We were told that the BlueCross BlueShield health insurance plans and the Medicare program frequently use this method. This representative also said that insurers and providers frequently match records among themselves, using SSNs to determine whether individuals have other insurance. This allows insurers to coordinate payment of insurance benefits.

Officials in the health care industry expect their use of SSNs to increase. Because health care services are generally delivered through a coordinated system that includes health care providers and insurers, it is important for health care providers to be able to accurately identify information about patients. However, health care providers may also use SSNs to gather information that is not directly relevant to a patient's health care. For example, one hospital official said that her hospital plans to use SSNs during the admission process to obtain on-line verification of patients' addresses.

Financial Services Businesses

Three national credit bureaus serve as clearinghouses for consumer credit reports and receive information about consumers' credit card transactions and payments from businesses that grant consumer credit. Officials from a bank and a credit card company told us that banks and credit card companies voluntarily report customers' payments and credit card transactions, accompanied by SSNs, to credit bureaus. They do so because ensuring that credit bureaus have

up-to-date consumer payment histories serves the interest of companies, like themselves, that provide credit. An official for a credit bureau trade association estimated that each national credit bureau has more than 180 million credit records. SSNs are one of the principal identifiers credit bureaus use to update individuals' credit records with the monthly reports of credit and payment activity creditors send them. In addition, credit bureaus use SSNs that are provided by customers to retrieve credit reports on individuals. Credit bureau officials told us that customers are not required to provide SSNs when requesting reports, but requests without SSNs need to include enough information to identify the individual.

Businesses such as insurance companies, collection agencies, and credit grantors use SSNs to request information about customers from credit bureaus. Banks and credit card companies in particular want information on customers' histories of repaying debts and whether customers have filed for bankruptcy or have monetary judgments against them, such as tax liens. Officials representing credit grantors said most banks and credit card companies ask applicants to provide their SSNs, and these credit grantors may choose to deny services to individuals who refuse. These officials said that their organizations generally do not use SSNs as internal identifiers but instead assign an account number as a customer's primary identifier.

Businesses That Sell Personal Information

Continuing advances in computer technology and the ready availability of computerized data have spurred the growth of information brokers who amass and sell vast amounts of personal information, including SSNs, about members of the public. One official from a firm that sells information told us that his organization has more than 12,000 discrete databases with information about individuals. Federal law does not prohibit these businesses from disclosing SSNs.

Brokers buy and sell information from and to a variety of public and nonpublic sources. Examples of the information they buy include public records of bankruptcy, tax liens, civil judgments, real estate ownership, driving histories, voter registration, and professional licenses. The information broker's purchase may include SSNs. Some brokers sell information only to businesses that establish accounts with them; others sell it to anyone. Law firms, law enforcement agencies, research organizations, and individuals are among those who use brokers' services. For example, lawyers, debt collectors, and private investigators may request information about an individual's bank accounts and real estate holdings for use in divorce or other civil proceedings; automobile insurers may want information about whether insurance applicants have been involved in accidents or have been issued traffic citations; employers may want background checks on new hires; pension plan administrators may want information to locate pension beneficiaries; and individuals may ask for information to help locate their birth parents.

To meet the needs of the parties to whom they sell information, information brokers have databases that can be searched by identifiers that may include SSNs; brokers may also include SSNs along with the other information they provide to customers. When possible, information

brokers retrieve data by SSN because it is more likely than other identifiers to produce records for a specific individual.

BUSINESS AND STATE OFFICIALS BELIEVE FEDERAL LAWS RESTRICTING USES OF SSNs WOULD HAVE A NEGATIVE EFFECT ON THEIR ACTIVITIES AND PROGRAMS

Officials from the businesses and agencies we contacted told us that federal restrictions on using SSNs could hamper their ability to conduct routine internal activities and their ability to exchange data. For each of these entities, correctly matching a specific individual to a corresponding record of information is an important concern. Consequently, these officials told us, federal limits on the use of SSNs could adversely affect their activities and programs. They told us that limits on the use of SSNs, for example, would lessen the certainty with which credit information could be matched to specific individuals and hinder health care service providers' ability to track patients' medical histories over time and among multiple providers. They also told us that such action could impede state tax agencies' ability to identify those who file taxes, make it difficult to associate tax return information received from other tax agencies with tax information reported by residents, and make it more difficult for states to link driver license applicants to traffic violations they may have acquired under other state licenses. Finally, officials from state agencies that license drivers told us that if they could not use SSNs to query their databases, it would increase the likelihood that government and law enforcement agencies would receive the records of multiple people with the same name when they requested information about a particular individual.

Because of privacy concerns raised by the disclosure of personal information, some businesses and states have voluntarily restricted their disclosure of such information, including SSNs. In December 1997, 14 of the self-identified industry leaders of those businesses that sell personal information voluntarily agreed to make the SSNs they obtain from nonpublic sources available only to a limited range of customers. They identified such customers as those having appropriate uses for this information, such as law enforcement. Although these brokers agreed to limit their disclosure of SSNs obtained from nonpublic sources, it should be noted that most of the SSNs they acquire come from public sources, according to an official from an information brokerage company. As part of their agreement regarding disclosure of SSNs, the 14 organizations also agreed to annual compliance reviews by independent contractors. If an organization fails to comply with the agreement, the Federal Trade Commission can cite the organization for unfair and deceptive business practices. The agreement became effective on December 31, 1998. Recent reports indicate that the first round of compliance reviews is complete and all of the companies have generally complied with the agreement.[4]

In addition to the voluntary efforts of businesses, some states are discontinuing practices that result in routine disclosure of SSNs. For example, since July 1, 1997, Georgia no longer automatically prints SSNs on licenses but rather assigns its own numbers for driver licenses and uses the SSN as a license number only if requested by the license holder to do so. Ohio, which

[4]One company no longer offers products that fall within the scope of the agreement.

before July 29, 1998, routinely printed SSNs along with state-assigned numbers on driver licenses, now allows drivers the option of not having SSNs printed on their licenses. Also, AAMVA officials believe most states in which driver records are public now exclude SSNs when responding to requests for driver records.

Finally, SSA has stated that the expanded use and misuse of SSNs poses an administrative burden for the agency. According to agency officials, widespread use of SSNs as identifiers requires SSA to meet more requests for SSN verification from employers and government agencies. In addition, the disclosure of SSNs increases those instances in which the agency must issue individuals new SSNs when theirs are being misused by another party.

CONCLUDING OBSERVATIONS

In conclusion, the widespread use of the SSN is permissible under existing laws and regulations, but because it provides a means to build and share databases of personal information, it creates privacy concerns and enables the growing problem of identity theft. The Congress must weigh such concerns about individual privacy and confidentiality of sensitive data against the government's need for timely and accurate information to control payments and prevent fraud and abuse in its benefit and loan programs. Moreover, limiting the use of SSN's in the commercial sector could slow or hamper some of the benefits of information sharing, such as speedy processing of applications for loans or credit. Although such restrictions could reduce identity theft, in our increasingly electronic world, protecting privacy will continue to be a public policy challenge.

Mr. Chairman, this concludes my prepared statement. At this time, I will be happy to answer any questions you or other Members of the Subcommittee may have.

- - - - -

GAO CONTACT AND STAFF ACKNOWLEDGMENTS

For information regarding this testimony, please contact Barbara Bovbjerg at (202) 512-7215. Individuals who made key contributions to this testimony include Kay Brown, Jacquelyn Stewart, and Roger Thomas.

(207100)

Mr. HORN. Thank you very much.

We now have our second witness, Hon. Fritz Streckewald, Associate Commissioner for Program Benefits in the Social Security Administration, which most know is an independent agency that reports directly to the President.

Mr. STRECKEWALD. Thank you, Mr. Chairman and members of the subcommittee, for inviting the Social Security Administration to testify on H.R. 220, the Freedom and Privacy Restoration Act of 1999, a bill designed to limit the use of the Social Security number [SSN].

I will submit my full statement for the record and summarize my remarks.

At the outset, let me emphasize that SSA has always taken its responsibility to protect the privacy of personal information in agency files very seriously. For almost 65 years, SSA has honored its commitment to the American people to maintain the confidentiality of the records in our possession. We have longstanding and effective practices to maintain individuals' privacy.

Initially, the only purpose of the SSN was to keep an accurate record of the earnings covered under Social Security and to pay benefits based on those earnings. The Social Security card is a document SSA provides to show what SSN is assigned to a particular individual.

In spite of the narrowly drawn purpose of the SSN, use of the SSN as a convenient means of identifying people in records systems has grown over the years in steps often taken for good reasons, such as, in the public sector to help enforce laws, protect the public treasury, and collect funds from delinquent non-custodial parents.

My statement for the record summarizes how legislation enacted over the years has expanded this use. While there are concerns that expanded use of a SSN as an identifier can compromise personal privacy, there are those that believe that the public interest and economic benefits are well served by these uses of a SSN.

For instance, all Federal benefit-paying agencies rely on data matches to verify not only that the applicant is eligible for benefits, but also to ensure that the benefit paid is correct. The SSN is the key that facilitates the ability to perform the matches. We actively participate in data matches to ensure the accuracy of Federal and State benefit payments, to verify whether applicants are eligible for benefits, to undertake debt collection activities, and to safeguard program integrity.

For example, our data matches with Federal, State, and local prisons save the Social Security in the supplement security income programs about $212 million annually and our national matches of death records save about $240 million annually. In addition, we verify SSN for employers to ensure correct posting of wages and for other Federal benefit-paying programs to help reduce their program costs.

The data matching process is highly efficient, especially for programmatic benefits, which allows SSA to more quickly determine continuing eligibility and to ensure correct payment amount. SSA's estimated savings total about $700 million annually from computer matches for the Social Security and SSI programs and savings for

other Federal, State, and local programs total about $1.5 billion annually.

Mr. Chairman, SSA is very concerned that H.R. 220 would severely limit our ability to perform data matches and would restrict data exchanges which benefit the public. SSA and other Federal, State, and local governments use these data exchanges to ensure accurate payment of benefits and to verify eligibility. Limitations or foreclosures of such data exchanges would undermine SSA program integrity initiatives, cost about $2.2 billion in lost savings to Federal, State, and local government programs, and erode public confidence in SSA's stewardship of the SSA programs.

Even though there are attempts to provide an exception for Social Security use of the SSN, the language in the bill is not clear as to whether SSNs could be used as the Social Security claims number for benefits. It is also not clear as to whether the exception would apply to the use of the SSN for SSI purposes.

I understand that SSA's Inspector General, in a statement he is providing for the record at this hearing, has many of the same concerns about H.R. 220 that we have. We share Representative Paul's concerns about the expanded use of the SSN in every phase of society. However, at the same time, we have an obligation to ensure that benefits are paid only to eligible individuals and that the correct benefit is paid.

In conclusion, Mr. Chairman, by using data matching, SSA and other benefit-paying agencies validate that the correct amount is paid only for an eligible beneficiary. The expense of trying to obtain information from other agencies without a unique identifier would be prohibitive as well as labor intensive. In addition, we must carefully weigh the balance between protection of individual privacy rights and the integrity of the Social Security programs.

We look forward to working with you to find the right balance and I would be glad to answer any questions you may have.

[The prepared statement of Mr. Streckewald follows:]

FOR RELEASE UPON DELIVERY

H.R. 220
Freedom and Privacy Restoration Act

STATEMENT BY

FRITZ STRECKEWALD
ASSOCIATE COMMISSIONER FOR
PROGRAM BENEFITS

HEARING BEFORE THE HOUSE COMMITTEE ON
GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY

MAY 18, 2000

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting the Social Security Administration (SSA) to testify on H.R. 220, the Freedom and Privacy Restoration Act of 1999, a bill designed to limit the use of the Social Security number, or SSN. Today, I will discuss the original purpose of the SSN, and how its use has expanded over the years. I will also talk about what effect this expansion has had on SSA and the conditions under which we disclose or verify an SSN for third parties. In addition, I will discuss how the number facilitates the data matches used in program integrity to verify eligibility for and benefit amounts of Social Security, Supplemental Security Income (SSI), and other Federal and State benefits.

At the outset, let me emphasize that SSA has always taken its responsibility to protect the privacy of personal information in Agency files very seriously. When the Social Security program began, people were concerned that information they provided to Social Security could be misused. The Social Security Board, charged with implementation of the Social Security Act, issued press releases and public statements to provide reassurance that information provided by individuals and employers would be regarded as confidential and would be available only to the individuals to whom it pertains and to Government personnel who need access to carry out their official responsibilities.

Almost immediately, these broad pledges of confidentiality were translated into official binding policy when the Board published its first regulation in 1937. This pledge of confidentiality has been an important factor in the cooperation which employers and employees have shown over the years in providing required information.

For almost 65 years, SSA has honored its commitment to the American people to maintain the confidentiality of the records in our possession. We have longstanding and effective practices and procedures to maintain individuals' privacy.

Original Purpose of the Social Security Number and Card

To begin, I'd like to talk about the original purpose of the SSN and the Social Security card. Following the passage of the Social Security Act in 1935, the SSN was devised administratively as a way to keep track of the earnings of people who worked in jobs covered under the new program. The requirement that workers covered by Social Security apply for an SSN was published in Treasury regulations in 1936.

Initially, the only purpose of the SSN was to keep an accurate record of earnings covered under Social Security and to pay benefits based on those earnings. The SSN card is the document SSA provides to show what SSN is assigned to a particular individual. The SSN card, when shown to an employer, assists the employer in properly reporting earnings.

Growth of SSN as an Identifier for Other Federal Purposes

In spite of the narrowly drawn purpose of the SSN, use of the SSN as a convenient means of identifying people in records systems has grown over the years in steps often taken for good reasons such as, in the public sector to help enforce laws, protect the public treasury, and collect funds from delinquent non-custodial parents.

In 1943, Executive Order 9397 required Federal agencies to use the SSN in any new system for identifying individuals. This use proved to be a precursor to an explosion in SSN usage which came about during the computer revolution of the 1960's. The simplicity of using a unique number that most people already possessed encouraged widespread use of the SSN by Government agencies and private organizations as they adapted their record-keeping and business applications to automated data processing.

In 1961, the Federal Civil Service Commission established a numerical identification system for all Federal employees using the SSN as the identifying number. The next year, the Internal Revenue Service (IRS) decided to use the SSN as its taxpayer identification number (TIN) for individuals. And, in 1967, the Defense Department adopted the SSN as its identification number for military personnel. Use of the SSN for computer and other record-keeping systems spread throughout State and local governments, and to banks, credit bureaus, hospitals, educational institutions and other areas of the private sector. At the time, there were no legislative authorizations for, or prohibitions against, such uses.

Statutory Expansion of SSN Use in the Public Sector

The first explicit statutory authority to issue SSNs did not occur until 1972, when Congress required that SSA assign SSNs to all aliens authorized to work in this country and take affirmative steps to assign SSNs to children and anyone receiving or applying for a benefit paid for by Federal funds. This change was prompted by Congressional concerns about welfare fraud and about noncitizens working in the U.S. illegally. Subsequent Congresses have enacted legislation which requires an SSN as a condition of eligibility for applicants for SSI, Aid to Families with Dependent Children (now called Temporary Assistance to Needy Families), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of any tax, general public assistance, drivers license, or motor vehicle registration law within its jurisdiction.

At the same time legislation was being enacted to expand the use of the SSN, Congress became concerned about the widespread use of the SSN as an identifier. As a result, the Privacy Act was enacted in 1974. It provides that, except when required by Federal statute or regulation adopted prior to January 1975, no Federal, State or local government agency could withhold benefits from a person simply because the person refused to furnish his or her SSN.

However, Congress continued to enact legislation that authorizes certain uses of SSNs in the public sector or required governmental agencies to collect the SSN, limiting the effect of the Privacy Act.

In the 1980's, separate legislation provided for additional uses of the SSN including employment eligibility verification, military draft registration, commercial motor vehicle operators licenses, and for operators of stores that redeem food stamps. Legislation was also enacted that required taxpayers to provide a taxpayer identification number (SSN) for each dependent age 5 or older. The age requirement was lowered subsequently, and an SSN is now required for dependents, regardless of age. The expansion of use of the SSN continued through the late 1980's with the requirement that an SSN be provided by applicants for Housing and Urban Development programs and authorizing blood donation facilities to use the SSN to identify blood donors.

In the 1990's, SSN use continued to expand with legislation that authorized its use for jury selection and for administration of Federal workers' compensation laws. A major expansion of SSN use was provided in 1996 under welfare reform. Under welfare reform, to enhance child support enforcement, the SSN is to be recorded on almost every official document an individual may obtain; e.g., professional licenses, drivers licenses, death certificates, birth records, divorce decrees, marriage licenses, support orders, or paternity determinations. When an individual is hired, an employer is required to send the individual's SSN and identifying information to the State which will verify the information with SSA. This "New Hire Registry" is part of the expanded Federal Parent Locator which enables States to find non-custodial parents by using the SSN.

Private Sector Use of the SSN

Unlike public sector use of the SSN, private sector use of the SSN is not specifically authorized but neither are there any restrictions. People may be asked for an SSN for such things as renting a video, getting medical services, and applying for public utilities. They may refuse to give it. However, the provider may, in turn, decline to furnish the product or service.

Officials from financial services companies advised the General Accounting Office (GAO) for their February 1999 report, "Use of the Social Security Number is Widespread," that, although they ask for an SSN, they generally do not use SSNs as internal identifiers but instead assign an account number as a customer's primary identifier. They expressed concern, however, that if prohibited from using an SSN, their ability to conduct routine internal activities and correctly match a specific individual to a corresponding record of information would be severely hampered.

The SSN as an Identifier

As you can see, Mr. Chairman, the current use of the SSN as a personal identifier in both the public and private sectors is not the result of any single step; but rather, from the gradual accretion over time of extending the SSN to a variety of purposes. The implications for personal privacy of the widespread use of a single identifier have generated concern both within the government and in society in general. Opposition to the use of such an identifier stems from the fear that it will be used improperly to exchange information among organizations or could possibly lead to dossiers about people which would follow them throughout life, make identity theft easier, or compromise a person's privacy.

The advent of broader access to electronic data through the Internet and the World Wide Web has generated a growing concern about increased opportunities for access to personal information. Some people fear that the competition among information service providers for customers will result in broader data linkages with questionable integrity and potential for harm.

On the other hand, there are some who believe that the public interests and economic benefits are well-served by these uses of the SSN. They argue that it would enhance the ability to more easily recognize, control and protect against fraud and abuses in both public and private activities. All Federal benefit-paying agencies rely on data matches to verify, not only that the applicant is eligible for benefits, but also to ensure that the benefit paid is correct. The SSN is the key that facilitates the ability to perform the matches.

SSA Verification Workload

SSA verification workloads relating both to use and misuse of the number have increased as the number's use has expanded. Such verifications are done primarily through regular automated data exchanges. We actively participate in data matches to ensure the accuracy of Federal and State benefit payments, to verify whether applicants are eligible for benefits, to undertake debt collection activities, and to safeguard program integrity. The SSN, as the common identifier, is the key to these matches. In addition, we verify SSNs for employers to ensure the correct posting of wages and for other Federal benefit-paying programs to help reduce their program costs. Where required by law and, in certain circumstances where permitted by law, we verify that the name and SSN in the files of third parties are the same as those on our SSN records.

Examples of disclosures or verifications we perform required by statute include:

- to the Office of Personnel Management for the purpose of administering its pension program for retired Federal Civil Service employees;
- to the Immigration and Naturalization Service to identify and locate aliens in the United

States;

- to the Department of Education for verifying the SSNs of student loan applicants;
- to the Department of Veterans Affairs to determine eligibility for, or amount of, veterans benefits; and
- to State agencies and courts to locate absent parents owing child support.

Disclosures we make that are permitted by the Privacy Act include:

- to the Department of Justice for investigating and prosecuting violations of the Social Security Act or for litigation involving SSA components or employees;
- to the Department of Treasury for tax administration and for investigating the alleged forgery or unlawful negotiation of Social Security checks; and
- to Federal, State and local entities for the purpose of administering income maintenance and health maintenance programs, where use of the SSN is authorized by Federal statute.

Matches for Program Integrity Purposes

We rely on data matches to verify eligibility factors, that is, that the applicant is eligible for the benefit, to protect the integrity of our programs, and for debt collection activities. Use of the SSN facilitates our ability and that of other agencies to perform the matches. Many of the data matches are mandated by statute, such as the State death data match which provides State death certificate information to SSA, as well as providing death data to other benefit-paying Federal agencies for them to determine if recipients are fraudulently claiming benefits. We also do matches for prisoner reporting which provides information on incarceration so that SSA can suspend benefits.

While these data matches are invaluable to us, nothing is more important in the operation of our programs than ensuring that the public has confidence that the information placed in our trust is secure. This is a cornerstone of our philosophy. SSA uses state-of-the art encryption software that protects data sent to us and systems firewalls that protect access to our databases. We are constantly reevaluating the security features necessary to protect the information we receive and maintain.

How Does Matching Work?

SSA computer matching, as is true for matching by other Federal and State agencies, is regulated by the Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act. The Act prescribes a procedural framework for matching activities, to include mandatory provisions that an individual be provided due process before a benefit is denied or terminated, that appropriate safeguards are adopted to preserve the confidentiality of the data

being exchanged, and prohibitions on duplication and redisclosure of the data other than for purposes covered by the match.

Because of our overriding concern for the confidentiality of the personal information in our records, and as required by the Computer Matching and Privacy Protection Act of 1988, SSA establishes an agreement with another agency to conduct computer matches for a specified purpose. This agreement is specific as to what the receiving agency can do with the information it receives from SSA.

A computer comparison of an entire non-SSA database of information is matched against an entire SSA database (e.g., all Federal Workers Compensation cases compared to all disability beneficiaries). The computer compares the records for discrepant information, and may also identify characteristics of highly suspicious cases. After the computer comparison discovers discrepancies, an alert is sent to an SSA employee to investigate. The employee notifies the beneficiary, advising him or her that information produced by matching may disqualify the individual from receiving benefits or result in a reduction of benefits, but no adverse action will be taken until he or she has had an opportunity to contest the information. Only after due process has been satisfied will SSA take action, if warranted, to change the benefits.

This process is highly efficient for programmatic benefits and allows SSA to quickly determine eligibility and ensure correct payment amount. Our computer matches comply with the due process, notice and individual privacy safeguards required by the Computer Matching and Privacy Act of 1988. SSA estimates savings to the trust funds of $332 million annually from computer matches for title II benefit purposes.

In order to improve the payment accuracy rate in the SSI program, designated by the General Accounting Office (GAO) as a "high risk" program, we are pursuing improved matching of our data with available records on wages, nursing home admissions, and financial accounts. GAO recommended that data matches were an effective means of reducing overpayments in the SSI program. In response to the recommendations, Congress included in the Foster Care Independence Act of 1999 (enacted on December 14, 1999) authority for SSA to conduct certain matches to capture information that directly affect eligibility and payment amount. The SSN is the key to those data matches. Matching information with various databases holds great promise in preventing SSI overpayments in these areas. Access to such data is vitally important in our efforts to strengthen the management of the SSI program.

Our actions are already showing results. For example, the data matches performed in FY 1999, along with other improvements, are projected to result in substantial savings in overpayment collection and prevention for the SSI program at a comparatively low administrative cost. In FY 1999, SSA saved almost $700 million in both title II and title XVI by sharing data with other Federal and State agencies. Similarly, according to agency estimates, other Federal, State and local agencies also saved about $1.5 billion.

SSA and many other Federal agencies use data sharing for three of the most important debt collection tools. The debt collection tools provided for under the Debt Collection Improvement Act of 1996 that rely on data sharing are: Tax Refund Offset where SSA refers delinquent debts to Treasury; Treasury Offset Program which expands offset to government payments other than tax refunds; and Credit Bureau Reporting where delinquent debtors are reported to Equifax and Trans Union.

Public concern over the availability of personal information has encouraged some to consider ways to limit using SSNs to disclose such information. However, GAO's February 1999 report on the widespread use of the SSN indicates that officials from both private businesses and State governments have stated that if the Federal government passed laws that limited their use of SSNs, their ability to reliably identify individuals' records would be limited as would their subsequent ability to administer programs and conduct data exchanges with others.

H.R. 220

Which leads to my discussion of H.R. 220. Let me begin by briefly summarizing the provisions that affect SSA. The stated purpose of H.R. 220 is to prohibit the use of the Social Security number as an identifier.

Specifically, the bill would:

- amend title II (Old Age, Survivors and Disability Insurance) of the Social Security Act and the Internal Revenue Code to prohibit any Federal, State, or local government agency or instrumentality from using a Social Security number or any derivative as the means of identifying any individual, except for Social Security and certain tax purposes.

- amend the Privacy Act of 1974 to prohibit any Federal, State, or local government agency or instrumentality from requesting an individual to disclose their Social Security account number on either a mandatory or a voluntary basis except for Social Security and tax purposes.

- prohibit any two Federal agencies or instrumentalities from implementing the same identifying number with respect to any individual, except for Social Security and tax purposes.

- prohibit a Federal agency from establishing a uniform standard for identification of an individual that is required to be used by any other Federal agency, State agency, or a private person for any purpose other than the purpose of conducting the authorized activities of the Federal agency.

- prohibit a Federal agency from establishing a uniform standard for identification of an individual that is required to be used for a purpose to which the Federal Government is not a party; or for administrative simplification.

Conclusion

Mr. Chairman, H.R. 220 would severely limit SSA's ability to perform data matches. The bill would restrict data exchanges which benefit the public. SSA and other Federal, State and local governments use these data exchanges to ensure accurate payment of benefits and to verify eligibility. Limitations or foreclosure of such data exchanges would undermine SSA program integrity initiatives, cost about $1 billion in lost savings, and erode public confidence in SSA's stewardship of Social Security programs. Even though there are attempts to provide an exception for Social Security use of the SSN, the language is not clear as to whether the SSN could be used as a Social Security claim number for benefits. It is also not clear as to whether the exception would apply to use of the SSN for SSI purposes.

In conclusion, I want to reiterate SSA's longstanding and ardent protection of the confidentiality of the personal information in our records. We share Representative Paul's concern about the expanded use of the SSN in every phase of society. However, at the same time, we have an obligation to ensure that benefits are paid only to eligible individuals and that the correct benefit is paid.

The way for SSA and other benefit paying agencies to validate that a benefit in the correct amount is paid only to an eligible beneficiary is to verify the information he or she provided. Without a unique identifier, trying to obtain information from other agencies would be cost-prohibitive, as well as, labor intensive.

In the use of SSNs, we must carefully weigh the balance between protection of individual privacy rights and the integrity of the Social Security programs and other benefit paying programs. We look forward to working with you to find the right balance.

I will be glad to answer any questions you may have.

Mr. HORN. Thank you for that statement.

Now we lean to a scholar in the field on this subject, and that is Dr. Charlotte Twight, the professor and privacy expert, Boise State University.

Welcome.

Ms. TWIGHT. Thank you.

Good afternoon, Chairman Horn and members of the subcommittee. Thank you very much for inviting me to testify today.

In addition to my written statement, I also request that a copy of my article entitled, "Watching You: Systematic Federal Surveillance of Ordinary Americans," distributed last November to each Member of the House by Congressman Ron Paul, be included in the hearing record.

Mr. HORN. Without objection, the referenced article will appear in the record.

Ms. TWIGHT. Thank you.

I strongly support the spirit and the purpose of H.R. 220. My research suggests that without new measures such as H.R. 220 that significantly roll back the Federal quest for centralized information about American citizens, programs currently underway will inexorably tighten Federal monitoring and therefore control of American citizens.

Today the Social Security number [SSN], has become the key to detailed Government portraiture of our private lives. federally mandated SSN-linked databases now incorporate detailed information on every individual's employment, medical history, educational experiences, and finances, right down to each check that every person writes. Even the Secretary of Health and Human Services now describes American SSNs as a de facto individual or personal identifier.

SSNs were not supposed to be used in this fashion. They were supposed to be mere account numbers denoting an individual's old-age insurance account within the Social Security program. But expansion of SSN use came quickly. President Franklin D. Roosevelt began in 1943 by requiring all Federal departments and agencies that wanted to create records identifying individuals to utilize exclusively the Social Security account numbers.

But the full impact of Roosevelt's order was not felt until the 1960's when gradual computerization made SSN-based record systems increasingly appealing. The IRS began using SSNs as taxpayer identification numbers in 1962. The SSN became the Medicare identifier in the 1960's. And thereafter SSN use spread unabated.

As William Minor, writing the Columbia Journal of Law and Social Programs, described it: "By the 1970's, the SSN floodgates had opened fully. Congress in 1972 amended the Social Security Act to require the use of SSNs for identifying legally admitted aliens and anyone applying for Federal benefits. In the following years, additional legislation required the SSN for the identification of those eligible to receive Medicaid, AFDC benefits, food stamps, school lunch programs, and Federal loans."

Moreover, the 1970's Bank Secrecy Act required all financial institutions to identify customers by SSNs and preserve detailed

records of their customers' personal checks and other financial transactions.

The Privacy Act of 1974 did not stop the flood. Incrementalist policies continued to advance SSN use, as illustrated by the gradual introduction of requirements for Social Security numbers for young children. For approximately 50 years of the Social Security program, one did not acquire a Social Security number until beginning one's first job, usually around age 16. Today, as you know, every child must acquire a SSN at birth or shortly thereafter. That process culminated in 1996 when Congress passed a requirement that a SSN must be presented for anyone of any age claimed on Federal tax forms as a dependent.

In addition, as part of the 1996 Welfare Reform Act, the Federal Government mandated creation of a SSN-based Directory of New Hires at both the national and State level, covering every working individual in America who enters the work force or changes jobs. Privacy concerns raised by these developments are further magnified by recent Federal commitment to establish a national electronic database tracking each person's personal medical history and new Federal powers to track every child's educational experiences through a variety of Federal entities.

My research indicates that unless H.R. 220 or similar legislation is passed, the coordinated Government effort now underway to require even greater use of SSNs will further centralize Federal monitoring of all American citizens. This effort includes Federal mandates governing State drivers' licenses and birth certificates, Federal work authorization databases, Federal development of a unique health identifier for each American, Federal implementation of expanded education databases, and finally Federal development and issuance of new tamper-resistant Social Security cards, perhaps with biometric identifiers, viewed by many as a precursor of the long-feared national identity card.

Moreover, with the SSN now at the heart of a vast array of Government databases, linkage of those separate databases occurs routinely despite periodic statutory lip-service to individual privacy.

Against this backdrop, H.R. 220, in my view, is an important step in the right direction. It would repeal many of the privacy-eroding uses of SSNs that I have described this afternoon. I have made several specific suggestions in my written statement aimed at closing some loopholes that may exist in the bill's present language.

In my view, we are at a crossroads. Today, many people are so accustomed to massive Government monitoring of their lives that all too often they ask, why should people worry about Government monitoring if they haven't done anything wrong? That current and prospective levels of Federal monitoring of American citizens are incompatible with the ideas of freedom upon which this country was founded never crosses their minds.

Pervasive Government extraction of personal data, stored and linked via compulsory use of SSNs, is today's reality. The threat to privacy is clear. And in the absence of privacy, political and economic freedom cannot long endure. The restrictions contained in H.R. 220 represent our first real chance to counteract the erosion

of privacy that has taken place through the burgeoning use of SSNs.

In supporting H.R. 220, however, let us not forget that the ultimate solution to the existing Government threat to personal privacy is restricting the power of Government to interfere in people's lives. The quest for information about private citizens, after all, is a byproduct of the vast substantive powers now wielded by the Federal Government. Dr. Richard Sobel of Harvard Law School has stated that centralized information is centralized power. I would add that the converse is also true: with today's technology, centralized power is centralized information. With its fine existing provisions and the modifications I have suggested in my written statement, H.R. 220 perhaps can be a first step in reducing both centralized information and centralized power.

Thank you very much.

[The prepared statement of Ms. Twight follows:]

May 18, 2000

Congressman Stephen Horn, Chairman
Subcommittee on Government Management, Information, and Technology
Committee on Government Reform
U.S. House of Representatives

Testimony: Written Statement

Dr. Charlotte Twight, Professor of Economics, Boise State University

Hearing on H.R. 220, "Freedom and Privacy Restoration Act of 1999"

Chairman Horn and Members of the Subcommittee, thank you for inviting me to testify regarding H.R. 220, the Freedom and Privacy Restoration Act of 1999. I am a professor of economics at Boise State University, where I have taught since 1986. I hold a Ph.D. in economics as well as a law degree, both from the University of Washington in Seattle, and I am a member of the Washington State Bar Association.

I am submitting this statement in support of H.R. 220, whose spirit and purpose I strongly endorse. I will briefly describe the history and impact of the expanding use of Social Security numbers (SSNs) in the U.S., and then offer several specific suggestions regarding the provisions of H.R. 220. The history of SSN use presented below is adapted from my article "Watching You: Systematic Federal Surveillance of Ordinary Americans," published in *The Independent Review* (Vol. 4, No. 2, Fall 1999, pp. 165-200) and distributed last November to each member of the House by Congressman Ron Paul. I ask that the full text of that article, an electronic copy of which has been included with this statement, be reproduced in the hearing record.

Today the Social Security number has become the key to detailed government portraiture of our private lives. Even the Secretary of Health and Human Services (HHS) now describes American Social Security numbers as a "*de facto* personal identifier." Kristin Davis, senior associate editor for *Kiplinger's Personal Finance Magazine,* recently described "the growing use of social security numbers as an all-purpose ID" as the "single biggest threat to protecting our financial identities."

SSNs were not supposed to be used in this fashion. They were supposed to be mere account numbers denoting an individual's "old-age insurance account" with the Social Security Administration. But expansion of SSN use came quickly. President Franklin D. Roosevelt began the process in 1943 with his executive order requiring all federal departments and agencies that wanted to create records identifying individuals to "utilize exclusively the Social Security Act account numbers."

But the full impact of Roosevelt's order was not felt until computers became available. Gradual computerization made SSN-based record systems increasingly appealing throughout the 1960s. In 1961 the Civil Service Commission first ordered use of SSNs to identify all federal employees. The Internal Revenue Service (IRS) began using SSNs as taxpayer identification numbers in 1962. Department of Defense military personnel records were identified by SSN beginning in 1967; the SSN also became the Medicare identifier in the 1960s. Thereafter SSN use spread unabated. As William Minor, writing in the *Columbia Journal of Law and Social Problems*, described it:

> By the 1970s, the SSN floodgates had opened fully. Congress in 1972 amended the Social Security Act to require the use of SSNs for identifying legally-admitted aliens and anyone applying for federal benefits. In following years, additional legislation required the SSN for the identification of those eligible to receive Medicaid, Aid to Families with Dependent Children ("AFDC") benefits, food stamps, school lunch program benefits, and federal loans.

Moreover, the 1970 Bank Secrecy Act required all financial institutions to identify customers by SSN and preserve detailed records of their customers' personal checks and other financial transactions.

As you know, the Privacy Act of 1974 did not stop the flood. Incrementalist policies continued to advance SSN use, as illustrated by the gradual introduction of requirements for Social Security numbers for young children. For approximately the first fifty years of the Social Security program, one did not acquire an SSN until beginning one's first job, usually around age sixteen.

Today every child must acquire an SSN at birth or shortly thereafter. How was this radical change accomplished? Much as one conditions dogs: a bit at a time--and always with a reward attached. First, Congress required by statute in 1986 that every child claimed as a dependent on federal tax forms have an SSN by age 5. Then in 1988 Congress reduced it by statute to age 2; in 1990 Congress reduced it to age 1. Finally, in 1996, Congress passed a requirement that an SSN must be presented for *anyone of any age* claimed on federal tax forms as a "dependent." No SSN, no federal tax exemption. In general, to obtain any federal benefit today, tax-related or otherwise, one must present the SSNs of all parties affected.

In addition, as part of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (the "welfare reform act"), the federal government has mandated creation of a SSN-based Directory of New Hires, at both the national and state level, covering every working individual in America who enters the workforce or changes jobs. Privacy concerns raised by these developments are further magnified by recent federal commitment to establish a national electronic database tracking people's personal medical histories and new federal powers to track our children's educational experiences through the National Center for Education Statistics and other federal bodies.

Unless H.R. 220 or similar legislation is passed, the coordinated government effort now under way to require even greater use of SSNs will further centralize federal monitoring of all American citizens. Its key elements include:

- federal mandates governing state drivers' licenses and birth certificates;
- federal "work authorization" databases covering all working Americans and keyed to SSNs;
- federal development of a "unique health identifier" for each American in implementing a national electronic database of private medical histories;
- federal implementation of education databases; and
- federal development and issuance of new "tamper resistant" Social Security cards, perhaps with biometric identifiers, viewed by many as precursor of the long-feared

"national identity card."

With the SSN now at the heart of a vast array of government databases, linkage of those separate databases occurs routinely despite periodic statutory lip-service to individual privacy.

Against this backdrop, H.R. 220 is an important step in the right direction. It would repeal many of the privacy-eroding uses of SSNs that I have described above. I offer the following suggestions regarding the wording of H.R. 220:

• **Private firms' use of SSNs**: Section 2 of H.R. 220 establishes important restrictions on governmental use of the Social Security account number. I ask that, as part of H.R. 220, you also explicitly prohibit private firms from using SSNs as a means of identifying individuals and, in addition, prohibit private firms from requesting or requiring an individual to disclose his SSN as part of a business transaction, unless such identification or disclosure is mandated by federal law. H.R. 220 should require that the Social Security Administration, perhaps acting in conjunction with the U.S. Department of Justice, vigorously prosecute such unauthorized uses of SSNs. These provisions, which might be included in Section 2(a) of H.R. 220, as part of the revised paragraph (C)(i), would strengthen other relevant provisions of federal law.

The rationale for these suggestions is that the public has become so accustomed to government-mandated use of SSNs that most people no longer resist when private firms demand their Social Security number for identification purposes, despite the threat to privacy involved. Today department stores, grocery stores, and other private firms routinely ask for and obtain SSNs as part of the most trivial market transactions.

• **Identifying numbers**: Section 4 of H.R. 220 prohibits government-wide uniform identifying numbers. I suggest broadening the bill's definition of "identifying numbers." In light of rapid technological changes increasing the feasibility of "biometric identifiers" that may pose even greater threats than alpha-numeric symbols, the current definition of "identifying numbers" in Section 4 of the bill may be too narrow. It would strengthen the bill to add a Section 4(b)(3) to include in the definition of the prohibited identifying numbers "any other identifier or new form of

personal identification (including, but not limited to, biometric identifiers) made feasible by advances in technology."

• **Non-disclosure of identifying numbers:** I also recommend adding a provision to Section 4 that would prohibit the disclosure, between government entities, of the identifying numbers used by particular federal agencies, state agencies, or political subdivisions of a state. It should prohibit establishment of cross-tabulations of identifying numbers across agencies. The rationale for this suggestion is that, if the identifying numbers used by one agency are disclosed to another, it becomes a simple matter to cross-tabulate the agencies' databases and thereby substantially undermine the objectives of H.R. 220. This would strengthen existing federal laws against government database matching such as the 1988 Computer Matching and Privacy Protection Act.

• **Loophole for "authorized activities"**: Section 5(a)(1) prohibits a federal agency from mandating standards for identification of individuals to be used by other government entities or by private persons "for any purpose other than the purpose of conducting the authorized activities of the Federal agency establishing or mandating the standard." It thereby implies that a federal agency may mandate use of a uniform identification standard if it is for the purpose of conducting its "authorized activities." In my view, this is too broad, since many abuses of federal identifiers could be alleged to fall under this rubric. I therefore suggest narrowing this language in section 5(a)(1).

• **Loophole for certain other government-established identifiers**: Section 5(b) prohibits government-mandated standards for identification of individuals, where the standard is for either one of two listed purposes: either regulating a transaction to which the federal government is not a party, or "administrative simplification." I suggest adding a new provision 5(b)(3) designed to incorporate other euphemistic justifications, besides "administrative simplification," which could be artfully employed to rationalize use of government-established identifiers that in fact are contrary to the objectives of H.R. 220.

• **Enforcement**: I recommend adding provisions to H.R. 220 that would impose

significant civil and/or criminal penalties for violations of the bill's restrictions. Given the ease of linking computerized databases in ways that would violate the intent of this bill, the powerful economic and political incentives that may exist to carry out such violations, and the difficulty of detecting violations, it is imperative that the penalties for such violations be severe.

Pervasive government extraction of personal data, stored and linked via compulsory use of SSNs, is today's reality. The threat to privacy is clear. The restrictions contained in H.R. 220 represent our first real chance to counteract the erosion of privacy that has taken place through the burgeoning use of SSNs.

In supporting H.R. 220, however, let us not forget that the ultimate solution to the existing government threat to personal privacy is restricting the power of government to interfere in people's lives. The quest for information about private citizens is a by-product of the vast substantive powers now wielded by the federal government. Dr. Richard Sobel of Harvard Law School has stated that "centralized information is centralized power." I would add that the converse is also true: with today's technology, centralized power is centralized information. With its fine existing provisions and the modifications I have suggested, H.R. 220 perhaps can be a first step in reducing both centralized information and centralized power.

Mr. HORN. Thank you very much. That is very helpful and we will have further dialog on some of that you have mentioned.

Mr. Smith—Robert Ellis Smith—is editor of the Privacy Journal. We are glad to have you here.

Mr. SMITH. Thank you, sir.

We have really worked ourselves into an illogical situation, I think, in our country where we are relying on the Social Security number as an authenticator of a person's true identity, yet it is no longer a private number. Either we have to rely less on that number as an authenticator, or we have to find a way to make it a confidential bit of information. Doing the latter is going to be highly unlikely and very difficult.

Congress contributed a lot to this dilemma; so I think it has a burden to come up with a solution. This bill, H.R. 220, is really commendable for its brevity and its simplicity.

I would like to do two things in my testimony: show that the bill will not be disruptive to governmental agencies and outline some of the objections that people have to being enumerated. Mostly people have said that they object to Social Security use because of "privacy," but I think the concerns are deeper than that.

First, universal identification, whether it is de facto as we are close to having now or whether it is required by law, simply gives too much discretion to those who are in authority to demand that one's papers be in order. That is the kind of domestic passport that we have disparaged in South Africa and eastern Europe.

Second, being known as a number, not a name, is dehumanizing and we pay a big price for that. When people feel that they are dehumanized, it makes brutality, violence, and criminality a lot easier to do. The best place to look is in a prison, which is a dehumanizing environment because a person is not known by the name of his or her choice.

We should also look to prisons for another lesson, too. That is an environment where everybody is positively identified by number and name, yet they are certainly environments of criminality, fraud, and other behaviors for other reasons that we are all aware of.

Look also to the military, where everybody is positively identified by name and by number. I am sure the incident of criminality, fraud, and the like is roughly equivalent to what it is in the nonmilitary world.

Next, many Americans have a fundamental religious objection to being enumerated that goes back deep in our history. I have just completed a book about the history of privacy in the United States and found that this goes back to colonial times and contributed to many of the early objections to census-taking.

Next we should realize that assigning surnames and assigning numbers to people has really been a means of social control throughout the history of not only this Nation but other countries as well. In fact, the introduction of surnames was a governmental invention, not a family invention.

I believe that the need to carry a Government I.D., which is what we are moving toward, would really remove the spontaneity of American life, the intellectual risk-taking, the informality that other cultures have come to envy in the United States. Since the

1990's, there have been very compelling, pragmatic reasons to why we have to protect Social Security numbers, and that is the epidemic of identity theft. And I use that term intentionally. It has become an epidemic. The spigot for Social Security number availability on the Internet and through so-called information brokers has been the "header information" phenomenon that you described.

Representative Paul's bill and Representative Kleczka's bill, taken together, would really chop the phenomenon of identity theft roughly in half. And that is the reduction in fraud that we should realize. We think of abandoning Social Security numbers as an invitation to increase fraudulent activity. In fact, it will have the opposite effect, I believe, and cut down on identity fraud.

Mr. Turner asked for victims. There are probably thousands of victims now of identity theft, including the former chairman of the Joint Chiefs of Staff and the present president of the Associated Press, both of whom were subject to identity fraud solely because a stranger got a hold of their Social Security numbers, something that would not have happened without this header information phenomenon that you outlined.

I would like to talk about some of the alternatives to Social Security numbers. There are lots of organizations that do quite well without using either Social Security numbers or any numbers whatsoever.

Back in the 1970's, IBM discontinued using a Social Security number as an employee identification number. They do use it for payroll purposes. Now, by law, higher education institutions in both Wisconsin and Arizona are prohibited from using the Social Security number as a student identification number. Stanford University, for instance, has used a unique number for many years without the Social Security number.

And the largest collector of information in the whole world, the Church of Jesus Christ of Latter Day Saints, does not use the Social Security number at all. It was once suggested to me that we should look to genealogists to try to figure out ways to keep track of people accurately without Social Security numbers because for most of that database there are no Social Security numbers.

Congress can help a lot by pushing the Government to look toward biometric identifying devices. This is essentially the matching of a physical aspect of a person to prove his or her identity positively. It would do away with the need for numerical identification, do away with a lot of personal information, intrusive forms—no more mother's maiden name, none of that—and I think it would be a much more less intrusive way of establishing identity, if it is done correctly.

And we shouldn't worry that Americans can't tolerate more than one identity number. Canadians for many years have had both the health identifying number and a social insurance number.

A couple of suggestions for the bill—and I am about to conclude—one is that State tax authorities ought to be authorized to use the Social Security number. That is a compatible purpose with the purpose for which it was originally submitted as a Federal taxpayer identification.

Second, I would hope that this bill would make clear that nothing can compel a family to require that a child 16 years or younger

must be enumerated. There are lots of coercive requirements in the Government to make this necessary. Now we have in the United States something that all of us thought would never happen: an enumeration requirement from birth. The Internal Revenue Service requires that in order to get a credit or deduction for a dependent, one must produce a Social Security number, even if that is an infant. And if the family happens to be on public assistance, there is a requirement that they have a Social Security number from birth so that many nurses in maternity wards now say they don't care about the name of the child, they simply want a Social Security number so that they can complete their paperwork.

Many people, like myself, simply have to do without the deduction because I am not about to decide for my children that they should be enumerated before they can do that on their own. And I don't think that ought to be necessary. I think we ought to have a prohibition against requiring children under the age of 16 from being enumerated.

Thank you.

[The prepared statement of Mr. Smith follows:]

Privacy Journal
AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE
PO Box 28577
Providence RI 02908

401/274-7861
privacyjournal@prodigy.net
www.privacyjournal.net

Robert Ellis Smith
Publisher

Testimony of Robert Ellis Smith
Publisher, Privacy Journal, and Attorney[1]

Before the Committee on Government Reform
Subcommittee on Government Management,
Information, and Technology
U.S. House of Representatives

On Governmental Uses of Social Security Numbers
And Alternatives

May 18, 2000

Over the past decade we have worked ourselves into an illogical situation that has caused disruption to the lives of many citizens and made the proper identification of citizens actually less efficient, not more efficient. The dilemma is that we are relying on a single number to authenticate the true identity of an individual, at the same time that we have made that number semi-public. The identifier is the Social Security number.

This makes it easy for an impostor to pose as another person, by authenticating identity by using the innocent person's identifier. This would not be possible if government agencies and private businesses (1) relied less on the Social Security number to authenticate someone's identity or took steps to assure that the number remains a confidential bit of information. Instead, government agencies and businesses do just the opposite: they rely almost exclusively on the SSN as an authenticating device and make it easy for strangers to obtain someone else's number.

HR 220

HR 220 is commendable legislation in its brevity and its simplicity. At first glance, it might appear to be disruptive of government agencies, but it is not. It will restore dignity to the status of American citizenship and actually have the effect of lessening fraud and false identity.

The bill does two things: It will retard the trend towards requiring a national ID number and it will require government agencies to use more care in identifying individuals and in authenticating their identities.

"Papers in Order" Mentality

"America stands as one of the few places where citizens have the freedom to travel without internal controls – and vast open space in which to exercise that freedom." I said that in 1991 when I testified on this subject before the Committee on Ways and Means on this same subject.[2] Since then we have allowed the government to coerce airlines into demanding photo identification from travelers, even on domestic flights, and so that unique freedom that I spoke of is no longer unfettered.

In writing my new book on privacy in American history,[3] I came across this revealing observation by a French writer in 1802 who marveled:

"From whatever part of the globe a person comes, he may visit all the ports and principal towns of the United States, stay there as long as he pleases, and travel in any part of the country without ever being interrupted by a public officer.[4]

If we do not reverse the trend towards a mandatory national ID number or document, we will have lost this freedom. It is the aspect of American society that foreigners most admire. It is the absence of this characteristic that we Americans disparage in other cultures: South Africa with its domestic passport until the 1990s; Eastern Europe during years of Communist control; and Nazi Germany, when it was always necessary "to have your papers in order."

A universal ID number or document – whether de facto or required by law – simply gives too much discretion to persons in positions of authority who stop and question innocent individuals pursuing innocent activities.

Dehumanization

Being known as a number, not a name, is also dehumanizing. It allows people in authority as well as our neighbors and co-workers to treat us as less than human. Prisons are dehumanizing because a person is not known by a name of his or her choosing. Consequently, in prisons, it is easy to brutalize other people. The more our culture dehumanizes our fellow citizens, the more we can expect anti-social, criminal behavior.

Religious and Philosophical Objections

Many Americans – mainly fundamentalist Christians – object to a governmental assignment of numbers for religious reasons. Under the First Amendment, that must be respected so long as those views, in the words of the courts, are "sincerely held."

It is up to individuals, not the state, to determine how individuals identify themselves. Throughout history, assigning surnames has been a government means for social control,[5] and assigning identity numbers serves the same purpose, with even greater control. When our founders were drafting our Constitution, governments in Austria and Prussia were just beginning to mandate last names.

Being required to present government ID or a government number at many points in our society removes the spontaneity of American life, the informality, the intellectual risk-taking, the freedom that other cultures envy.

Pragmatic Reasons

Since the early 1990s, there has been a strong pragmatic reason for protecting one's SSN: the epidemic of theft of identity. This epidemic has occurred since an unfortunate (and non-public) decision by the Federal Trade Commission in 1993 that credit bureaus may disclose or rent consumers' Social Security numbers and other identifying information "above the line" in a credit report. This means that "information brokers" or on-line "infomediaries" can easily purchase Social Security numbers and resell them on-line, often to anonymous buyers. Legislation to shut off this spigot, which leads to theft of identity nearly passed in 1996 and Rep. Kleczka has introduced similar legislation in this session (HR 1450).

Of course, the perpetrators of theft of identity have other sources of Social Security numbers – the hallways of universities where students grades are posted by Social Security numbers, trash in payroll offices, credit reports used at their places of employment, even the pages of the Congressional Record.[6] But HR 220 and HR 1450 together will reduce the problem of identity theft by 60 percent or more.

There are additional pragmatic reasons for this legislation. The incidents of inaccurate Social Security numbers are so numerous that any record linkage based on them will be seriously flawed. The SSNs is not totally anonymous; a stranger can tell from what state it was issued and approximately what year.

Alternatives to Use of SSNs

Limiting collection of SSNs will not be disruptive. With today's database technology, the SSN and other personal identifiers make using SSNs or any numerical identifiers unnecessary.

Using an algorithm to digitize a person's full name and other identifying information (birth date, address, occupation, or self-chosen PIN) keeps track of millions of data files in many organizations. Proprietary forms of this methodology include SOUNDEX, Alpha Search, and SearchSoftwareAmerica. Federal Express, the National Insurance Crime Bureau, VISA, and Wausau Insurance use variations of these techniques. The state of Maryland keeps track of millions of motor-vehicle files with these methodologies.

An additional advantage is that a search for a file using these methods will bring up several near matches, so that a clerk – or artificial intelligence in a computerized system – can select the accurate match. Thus, an error in one data element will still produce an accurate match. This is not true when data systems rely on one numerical identifier, like a Social Security number.[7]

Organizations like MIB Inc., which stores millions of computerized medical diagnoses on Americans for insurance companies, do not rely on Social Security numbers at all. Long ago, IBM discontinued using the number as an employee number. By law in Wisconsin and in Arizona, university systems must keep track of thousands of students without requiring a Social Security number.[8] For many years, Stanford University has used a unique lifetime Stanford University ID number, not the SSN. Genealogists keep track of millions of individuals without the benefit of any numerical identifiers. The Church of Jesus Christ of Latter-Day Saints (Mormon), which maintains the world's largest database of information about individuals, assigns a random ID number to each individual; it does not rely on Social Security numbers.[9]

Managers of most criminal justice information systems are smart enough not to rely on Social Security numbers to keep track of millions of computerized files on individuals.

Aside from technological alternatives, governmental agencies could comply with the bill simply by creating a randomly selected alternative ID number of nine digits for individuals who desire an alternative to a Social Security number.

Inaccuracy Rates

Let us not believe that Americans can be relied on to handle only one numerical identifier and that "everybody knows his or her Social Security number." In fact, studies show that many persons inadvertently provide an incorrect Social Security number from memory. Many people accidentally provide a spouse's number. Studies show a much higher accuracy rate when an individual has to consult a document when providing an identifying number, not relying on memory. The accuracy rate will undoubtedly be far higher if individuals present a machine-readable card for each discrete transaction – as they do for credit-card purchases.

For years, Canadians have had at least two identifying numbers – the Social Insurance Number (SIN) for the government-run pension system and a health-care identifier for each province's government-run health-care program. This is the way it should be in a democratic society – separate identifiers for separate purposes.

A single all-purpose number or identifier sounds convenient – until you think of the vast powers that this gives the people in charge of demanding the ID document.

Suggestions for the Bill

I suggest that the sub-committee consider adding to HR 220 a provision permitting state tax authorities to use the Social Security number as an individual taxpayer ID, because this is a purpose that is compatible with uses by the IRS authorized in the bill.

However, I suggest that the subcommittee make clear in the bill that there is an absolute prohibition against any government agency requiring a Social Security number for a child 16 years or younger, except for a child earning reportable income or desiring a Social Security number for employment.

There is time enough for each American to decide for himself or herself when and under what circumstances he or she will be labeled with a governmental number.

Prohibiting demands for SSNs on children would end (1) the IRS requirement that a Social Security number must be reported on Form 1040 for any child who is claimed as a dependent,[10] (2) the requirement that a Social Security number be secured for an infant if a family receives public assistance, (3) the coercion in many public school systems that children be enumerated by the Social Security Administration during the school day, and (4) the Department of Agriculture requirement that all members of a household must provide Social Security numbers if one member receives food stamps or reduced-price school lunches.

Each of these requirements, especially the Form 1040 requirement, has forced parents to get governmental ID numbers on their children at birth. The children, of course, have no opportunity to consent. They and their identifying numbers become part of governmental data systems from birth.

Thousands of parents like myself have declined to have their children enumerated in this way, and ought to be able to benefit from deductions and credits for their dependents if they can prove the existence of the child (and there is no suspicion that the child is claimed as a dependent by someone else).

---

[1] Since 1974, Robert Ellis Smith has published Privacy Journal newsletter, based in Providence RI. www.privacyjournal.net. He is the author of several books on privacy and has testified before Congress and state legislative bodies on different aspects of the issue. Privacy Journal has published "Report on the Collection and Use of Social Security Numbers" 1993).

[2] Subcommittee on Social Security, Committee on Ways and Means, February 27, 1991.

[3] Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Privacy Journal, Providence RI, 2000). One chapter in the book traces the history of Social Security numbers and the trend towards a national ID requirement.

[4] *Ben Franklin's Web Site*, page 307, quoting Francois Andre Michaux.

[5] James C. Scott, *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1998).

[6] Congressional Record, p. S2546, March 20, 1996, first reported in Privacy Journal, December 1996.

[7] Privacy Journal, July 1996.

[8] Wisconsin Statutes 118.169. Arizona Revised Statutes 15-183, Chap. 239, Laws of 1999.

[9] Privacy Journal, August 1996.

[10] 26 US Code 6676(e).

Mr. HORN. Thank you.

We will now proceed to some of the questions we have. Mr. Turner and I will divide it 10 minutes on a side each.

Let me start with the representative from the General Accounting Office.

You mentioned that most of the States give people the option of having another identifier on the drivers' licenses. How effective has that been in giving citizens added protection against fraud?

Ms. BOVBJERG. If I said most, I want to correct that because I am not sure that that is true. Some States do give people the option of having another number. And this is sort of an emerging position on the part of the States. We haven't assessed how extensive it is.

I think it is everyone's hope that not having it on your driver's license does help protect you from cashing a check and having someone take that number.

Mr. HORN. Has the separate identifier made it tougher for the Division of Motor Vehicles to keep track of the drivers?

Ms. BOVBJERG. That is among the many things we don't know about this.

Most States keep the Social Security number in some way, either on the license or they have linked it to this separate identity number for data matching with other States.

Mr. HORN. What is your judgment as to different alternatives of numbers that aren't the Social Security number? Is it just each person in an agency, or an agency and its personnel to start their own numbering system? What does GAO see as the relevant alternatives?

Ms. BOVBJERG. When I think about a system where each Federal program has a different system of numbering, one of the things I am concerned about is how you carry out your program stewardship responsibilities as the Federal Government. As the Social Security Administration stated earlier, there are a number of programs where data exchanges with other agencies help verify program eligibility or the level of benefit eligibility that people have. Without that, you are relying on self-reported information. Surely the overpayment cost would rise in such a situation.

Mr. HORN. But say—and this is a true situation—in my district there is a house in which 20 different people live and they all have the same name. How do you separate that out? And should you? And does it matter?

Ms. BOVBJERG. I think that it matters for certain types of uses. It matters to me, for example. My name didn't used to be so complicated. My name used to be Davis. And it mattered to me that I had a lot of difficulty cashing a check because I was constantly confused with all these Barbara Davises bouncing checks. So it might matter to an individual.

But that might differ among individuals as to how inconvenient that is. It matters a great deal to certain Federal programs that you have a unique identifier for an individual so that you can assign—in Social Security's case—their earnings to their account. In the IRS case, so you know they are paying their taxes and you are not looking at tax avoidance on the part of the wrong person.

There are a number of other Federal programs—I think we mentioned Pell grants earlier and student loans are another example.

Mr. HORN. This is an actual case. In the Eisenhower administration they were putting together a delegation to go to the International Labor Agency in Geneva. We found that people had exactly the same name, born in the same city in the State of New York, and had gone to school at the same time, and the interesting thing was that one was a communist and one wasn't. And yet that person who wasn't was going to be bounced because of this communist file, etc. And it wasn't somebody duplicating files or anything, it is just sheer chance.

So how do we solve that if we don't have something like a Social Security number that might help us differentiate between these people?

Ms. BOVBJERG. One of the things we have thought about—and we were thinking particularly of the private sector and less of the Federal Government— is that it would make their jobs harder if they couldn't use a unique identifier. But it does not make their jobs impossible. Now I am getting into a technological area that I can't go very far into, but then could we relational databases where you can look at a number of fields and, by combining them, create a unique identifier. But I am not sure that that is a comfort if the concern is protecting privacy and keeping personal information from being disseminated widely.

I think that in the private sector an inability to use the Social Security number will make things harder. It won't be as convenient for businesses. But they won't go out of business. There will be a way to figure out how to identify one Barbara Davis from another.

Mr. HORN. Would any of you like to comment on these questions and the answers? Does Social Security have a view on this?

Mr. STRECKEWALD. We are in agreement that without a unique identifier—as far as we know the Social Security number is the only unique identifier that is widely used—it is very easy to confuse John L. Smith of Lincoln Avenue with John L. Smith of Lincoln Boulevard. And for a lot of purposes—not only that you don't want Mr. Smith's credit on your credit account if you're not him—but also to make sure that we pay the right people. We agree that it would be very difficult.

The relational databases she is mentioning are feasible, but I think in the end they tend to do the same thing. You have to connect them so that you know who you're dealing with.

Mr. HORN. Any thoughts on this, Dr. Twight?

Ms. TWIGHT. One thought that I have is that when we are trying to weigh these things out, we are always going to have difficulty because the increased administrative costs associated with doing something other than having the Social Security number used as the all-purpose identification—those administrative costs are tangible and measurable.

The costs on the other side, in terms of loss of personal privacy, freedoms—those sorts of things, loss of personal autonomy—are by definition intangible and hard to measure. So I think that is an important thing to keep in mind when we are trying to balance these things out.

Mr. HORN. Mr. Smith.

Mr. SMITH. Historically, the Social Security Administration has had to deal with people who are using duplicate Social Security numbers and there are many people using more than one Social Security numbers. There are tie breakers, in the case of this home in California. There are—as the witness from GAO said—now techniques that we have that incorporate other aspects of a person's identity that we can use.

Nothing in Representative Paul's bill, first of all, prohibits the Social Security Administration from continuing to use that number. Nothing prohibits any Federal agency from using a unique identifier. What is prohibited is that they can't use the same one. I think that is doable.

Mr. HORN. How about having a modern type of reader for one's hands or fingerprints or whatever, but something so that when you go into a light there that apparently differentiates people. Presumably, then, the only people who might have it is your bank or something else. But it wouldn't be something that other people are likely to have without—it's hard to change your fingerprint.

Mr. SMITH. Exactly. And that is biometrics. And one of the values of it is that it tells only who you are. It tells nothing more about you. It doesn't tell how many kids you have or what you like to do at home. If implemented properly, it could be a less intrusive technique for establishing identity.

What we don't know at this point is the reliability rate. Most of them are no more than 60 to 70 percent as reliable as a fingerprint. Second, the real danger is that we will be tempted to use a DNA sample as the identifier, and that is an aspect that tells more about you than your identity. It will take in diseases and predilections for certain problems in the work place which could be extremely discriminating to people.

If it is implemented properly, I think biometrics is the less intrusive way to establish identity.

Mr. HORN. Any other reaction to that? Is biometrics——

Mr. STRECKEWALD. Mr. Chairman, for Social Security purposes, the Social Security number works very well. As long as we continually look to tighten our enumeration process, we feel that for Social Security purposes, for posting wages, for doing data matches with other Federal, State, and local governments that the Social Security number works fine. We are in the process of implementing recommendatins contained in a recent Inspector General report. And at this point, there is no need for biometrics.

The Social Security number was not meant to be an identifier. It only says that there is a number that relates to this person. It doesn't prove identity. Say that this person in front of you is necessarily that person. We use it for recordkeeping.

Mr. HORN. And you don't see any biometric that you could use?

Mr. STRECKEWALD. We haven't fully explored that yet.

Mr. HORN. Does GAO know about other Government agencies exploring that?

Ms. BOVBJERG. I don't. That would be something I could get back to you on.

Mr. HORN. If you would, I would appreciate it because I know I have looked at some of that equipment in various places and it could be used by Customs, Immigration, and so forth.

Ms. BOVBJERG. I know that HHS has looked at the possibility of Biometric Identifiers for purposes of the unique health identifier. That is one of the things listed in the report they came out with a while back. And I think that there are some questions and difficulties in terms of how much of a threat to personal privacy that will actually represent. I am not as sanguine about it as some of my colleagues here at the table.

Mr. HORN. Thank you for that comment.

I now yield 11 minutes to my colleague from Texas, the ranking member, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

I need some help on how you can calculate the cost of a piece of legislation like this. Obviously, if you're going to force the Federal agencies to abandon the use of the Social Security number, they are going to replace it with some other number. And I suppose that if you are against using an identifier, you might be against using any number. But I guess the problem I see is trying to figure out how you would accomplish this and at what cost would it incur.

Do any of you have any suggestions? Has GAO looked at this to see if there is any way you can estimate the cost of a bill like this?

Ms. BOVBJERG. Well, often we will ask CBO to do it.

But in this case I presumed that the bill prevents the Federal Government from coming up with any kind of replacement for a unique identifier. In considering the cost of the bill, I was actually thinking less about administrative costs than about the overpayment cost or the inability to collect on debt owed the Federal Government. And I think Dr. Streckewald has some figures on what Social Security and other agencies get from the current data matches they do. The cost could be something in that order of magnitude.

Mr. TURNER. What information do you have, Dr. Streckewald?

Mr. STRECKEWALD. Mr. Streckewald—thanks, though. [Laughter.]

Yes, that is how we have looked at this. We have no idea what it would cost to manually match notices. But we do know what we save from data matches.

Social Security is both the recipient and the source of numerous data matches. We save about $350 million a year from Title II data matches that we sent out daily to other agencies to verify income sources that Title II beneficiaries have. And we save about $350 million there.

We save another $325 million from the SSI Program doing the same thing, sending out data and getting it verified. We have been heard and there have been estimates within the agency that about $1.5 billion a year are saved by the State, local, and Federal Governments that send us information to verify and we verify the Social Security amount.

So there is a lot of money involved, $2.2 billion total just in the matches.

We are also concerned about our ability to collect debt. There are three tools that we use that we think this bill may jeopardize: the tax refund offset, which we use to offset refunds if people get to pay back their overpayments; the treasury offset program, which is

broader than just going to tax refunds; and then referring or reporting to credit bureaus delinquent debt.

In 1999, we collected $84.4 million using these techniques and we aren't sure if they would be available to us in the passage of this bill.

Mr. TURNER. Mr. Smith, wouldn't there be some way to continue to use the Social Security number because so many businesses are using it, and so many Government agencies are using it—but in areas where we want to be sure we protect access to the data that is identified by the Social Security number, we add some additional number as a part of the Social Security number—would that be helpful rather than simply abandoning the use of the Social Security number?

Mr. SMITH. I don't think this bill does abandon the use of it. It seems to me it coerces Federal agencies to use different identifying numbers.

A couple of ways, if you find the costs are too much—simply giving an option, the way the Privacy Act does, that an individual may not be declined benefits because of a refusal to give a Social Security number. Perhaps for 10 percent of your database you are going to have people with other nine-digit numbers assigned at random. I don't think that is unduly costly.

Another way, possibly, is to fix the language in the current bill that says you can't use a derivative of a Social Security number. Just using the last four digits with other randomly assigned numbers, Federal agencies can use it as a tie-breaker and can establish identity without sacrificing privacy. Agencies ought to look into that, too. That is another very real possibility.

Among the savings in cost will be a reduction in identity theft by 50 percent. That is mostly a private sector cost, but it's growing more and more. And you will save money from a lot of false matches. The Veterans' Administration finds a lot of false matches when they run a match based on a Social Security number. People quite often misstate one digit and that gives you a false match. And that is a very costly process to unravel that. So you will save that money as well.

Mr. TURNER. The first suggestion you made was basically to give an individual the option of whether they use the Social Security number.

Mr. SMITH. Yes.

Mr. TURNER. I can understand from an individual's perspective that that gives that person the option of trying, in that way, to preserve their privacy. But it seems like we ought to be dealing with this issue on a little broader basis. If it is important to protect the privacy of one person, it seems that it ought to be important to protect the privacy of all. So just to say that you are going to give people the option—which I would think would create a lot of confusion within the various agencies for people who say they don't want their Social Security number used—that you would be better off approaching this problem and being sure you are trying to institute and create ways to protect the privacy of everyone.

Mr. SMITH. You would protect the privacy of everyone if the option is available and it says in the law that you need not present the Social Security number if you wish not to. That would establish

for a lot of people the right to say no, which is essentially what they want. So it is not tailor-made just for a tiny few individuals. It is really how the Privacy Act provision on Social Security numbers was intended to work.

I recommend this only as an alternative. If it turns out that this is going to be an extremely costly endeavor—I don't think it is going to be a costly endeavor.

For instance, the State of Maryland manages all their motor vehicle records with no Social Security number at all. They use some of these modern techniques that I speak of.

Now, to convert to some of these other techniques—one of these is Soundex—there is going to be a cost, but I think the Federal Government is going to face that eventually. They are going to have to convert to those other identifiers because we can no longer rely on a system that relies on a Social Security number to authenticate your true identity and yet makes that number a public number. That just doesn't make sense.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. I just have a few questions to pursue, and here is one of them.

How does the Government account for people who refuse the Social Security number with regard to retirement benefits and Government services? What do we do on that?

Mr. STRECKEWALD. Social Security requires that you give us your Social Security number in order to receive benefits.

Mr. HORN. Do you know if private pension systems use that?

Mr. STRECKEWALD. I don't.

Mr. HORN. Did GAO look at that?

Ms. BOVBJERG. I believe that private pension systems would have to use it because of the tax affiliation. Private pensions are one of our largest tax expenditures.

Mr. HORN. Are you aware to what degree, say, IRS has problems with the members that don't have any Social Security number? Is that a problem with IRS?

Ms. BOVBJERG. It would be a problem not to have one, but I don't know what the extent of that problem is.

Mr. HORN. And then those that serve in the military, of course, does their dog tag include the Social Security number? Or do they just have their own?

I see nodding heads that they use their Social Security number.

Explain to me a little bit, Mr. Smith, the Soundex personal identification searcher. How does that work?

Mr. SMITH. Well, the way I understand it, it incorporates other factors in a person's name, address, birth date, even occupation, and makes it into essentially a digital formula. It can also be altered over time because one's address may change with time. It is, what I would call, a covert number. I never see it. It is simply a formula that identifies me. Whenever I present myself at an agency, they use the same algorithm to identify me.

The beauty of it is that when you have an applicant in front of you with name and perhaps birth date and address, you can retrieve the 10 or 12 closest matches and then either the computer or the individual can choose precisely the match you are looking

for. You can't do that with a Social Security number. If a person is one digit off, you aren't going to get a match.

So I think these modern techniques are more reliable in getting matches.

Mr. HORN. When we are talking about maybe rolling back the use of the Social Security number, is there any rational way you can think of to peel it back? And if so, where would you start, besides the Government?

Mr. SMITH. I would say it may be used only for Social Security purposes, its original intent, and tax purposes. One of the logics is chronological. Those were the first two. They were both established by law, not by Executive order or bureaucratic happenstance. They are closely allied purposes. They also now have become extremely ingrained and to stop those would be extremely disruptive. It would not be as disruptive to discontinue some of the other uses that have taken hold since the 1960's.

Mr. HORN. Any other thoughts on that and how we peel it back and which ones don't really need the number or could figure out another way to have a number of their own origin?

Have you taken a look at that, Dr. Twight?

Ms. TWIGHT. I agree with what Mr. Smith said.

Mr. SMITH. I think you identified the difficult question and that is Medicare. I am not prepared to answer that one. That is a tough one.

Mr. HORN. Especially when we think there is $30 billion of fraud there.

Mr. SMITH. Well, it is so closely allied with the Social Security system as well.

Mr. HORN. Exactly. There are interchanges there with Medicare and Social Security still?

Mr. STRECKEWALD. Yes, as far as I know.

Mr. HORN. Because they are under HHS and you're independent, you're still talking to each other?

Mr. STRECKEWALD. We sure are. We actually have some data matches with them, too.

Mr. HORN. What does GAO think about the peel back movement? Where would you start?

Ms. BOVBJERG. Well, when you were asking this, I was thinking—and I can tell you the exact name of the law in a minute—the Drivers' Privacy Protection Act seemed to have the potential to make some difference. That was just upheld by the Supreme Court a couple of months ago. It prohibits States from disclosing Social Security numbers for purposes like surveys, marketing, solicitation. They can no longer sell them as part of their motor vehicle drivers' license database without the express consent of the individual.

And it is too early to know whether that makes a difference, but it is data sets like that or birth certificates and things like that where the private sector sellers of personal information get the information that they sell.

Mr. HORN. Well, that's helpful and we will be asking other panels as to where they think they can peel this thing back a little bit and just not have everybody find out everybody else's Social Security number because it is getting to be pretty open.

In your survey, did a number of Federal agencies say they were using any individual identifiers or were thinking about it or what?

Ms. BOVBJERG. When we did our survey, we actually talked to States and private sector users. We didn't talk to Federal users in the same way. We talked more about what the laws require and what the restrictions were. So we didn't ask that question. Now that you're having this hearing, we wish that we had.

Mr. HORN. What about the States? We can look at them as a prototype of us. We are just a little bigger up here.

Ms. BOVBJERG. The States said that they would have trouble not using the Social Security number. A particular place is State taxes because they link their information to Federal tax information, Federal income information to try to do verification. They mentioned law enforcement as being an issue for them. I think in motor vehicles they would like to continue to use the number. They are still required to use the number for the commercial driver's license. But I think that was less of a concern to them than the law enforcement and tax enforcement areas.

Mr. HORN. Has any scholar ever done a book on what the Government was like before 1936 in terms of identifying people?

Ms. TWIGHT. Not that I am aware of.

Mr. HORN. It seems to me that would be a pretty interesting Ph.D. dissertation.

Mr. SMITH. Prior to 1935, very few people had a contact with the Federal Government so there weren't that many databases.

Mr. HORN. And that is one good reason why they didn't have it. It was a simpler world.

People cite technology as one of the vital factors in identifying theft and fraud. I am the author of the Debt Collection Act of 1996 and I have a letter here now from the general counsel of the Department of Treasury as to what the effect of Mr. Paul's bill would have on a lot of things such as debt collection. And that would bother me because there are a lot of people who are just chiselling the taxpayers. That is what got me started in that little endeavor.

A guy got a loan from the Farmer's Home Loan crowd and has this great ranch up in Sonoma County and then he defaults and they give him another loan to live in Santa Barbara, which is a rather pricey place, and there we are. We don't think the taxpayers' money should go that way.

Mr. SMITH. I would like to point out that characters like that also know to use different Social Security numbers; so we shouldn't rely on that number to catch crooks.

Mr. HORN. Before the technological revolution, personal information like Social Security would take an investigator weeks to obtain because none of the information was centralized. This is no longer the case. Information is in one central location or just a few keystrokes away.

Do you feel that is a realistic summation of the problem? That is just too easy now to find out so easily about people?

Mr. SMITH. Yes, definitely. The data systems are built and then privacy is an afterthought. Security is an afterthought, too.

Mr. HORN. Do you think it would be more effective to boost internal security on the distribution of the national identifier by Fed-

eral, State, and local agencies? Or what would you do to sort of limit that?

Mr. SMITH. When you have six to a dozen States that display it on the face of the license, I think the damage is done. You cannot put the Social Security number back into a confidential box, I am afraid. That is why a new identifier might have that potential. It could be truly a confidential bit of information that only the bearer would know.

Mr. HORN. Does anybody else have a comment on that approach?

Dr. Twight.

Ms. TWIGHT. I have a general comment. I wanted to share just two sentences from legal scholar, Paul Schwartz, who was writing in the Hastings Law Journal, "Personal information can be shared to develop a basis for trust, but the mandatory disclosure of personal information can have a destructive effect on human independence."

And he went on, "Totalitarian regimes have already demonstrated the fragility of the human capacity for autonomy. The effectiveness of these regimes in rendering adults as helpless as children is in large part a product of the uncertainty they instill regarding their use of personal information."

And then in the very next paragraph, he talks about how that has occurred in America to some degree, how people in America no longer know how their information is going to be used. And with these universal identifiers that we see represented now in the form of the Social Security number—it creates a lot of pressure for conformity that perhaps would not otherwise exist.

Mr. HORN. Any other comments?

Mr. STRECKEWALD. Mr. Chairman, I would like to respond to Mr. Smith's comment about systems being built without security in mind.

As you consider this bill, you need to also consider that Congress has seen fit to pass several laws that address this issue. The Computer Matching and Privacy Protection Act has a number of safeguards built into data matches, the type of things that are in question here. We have to specify the purpose of the match in a memorandum of understanding. We have to verify the information we derive from the match prior to acting on it. So we cannot lower someone's check just because the data match tells us that without verifying it.

We have to give the person an opportunity to contest the information. We have to have security procedures in place to protect the data, and we have to strictly limit redisclosure.

Social Security takes that even further. We personally go onsite and visit every agency that we share data with or from whom we get data to make sure that they have the security procedures in place and are capable of following this law.

Mr. SMITH. I would like to comment that that proves my point. Computer matching began in 1976 and 1977 and the bill came much later than that, in 1988. I was there at the creation. So first came matching and after came the security precautions.

Ms. BOVBJERG. I just have a couple of thoughts. One is that we have kind of been assuming that people's Social Security numbers are used entirely without their involvement. And it has been our

observation that people freely give out their Social Security number. I don't think people think about it very much anymore. It is difficult to keep such a thing confidential when people at various retail outlets ask for it and people give it to them.

The other thing I wanted to respond to is the idea of a new number that would be kept confidential. First, we would have to do a better job than we have done with people and how they safeguard their Social Security number. But my mind reeled as I thought of the prospect of how the Federal Government would actually accomplish this in any reasonable period of time—277 million people being re-enumerated. So there would be an administrative cost I would be concerned about.

Mr. HORN. But nobody has given us any. Does GAO want to make some guesses as to what the cost would be one way or the other?

Ms. BOVBJERG. We never guess at GAO. [Laughter.]

But I can tell you that anytime you do anything at the Social Security Administration that affects all cardholders, it costs a huge amount. We talked a year or so ago about the counterfeit-proof card and what it would cost to create such a thing. And the range was something like $4 billion to $10 billion. And that is because anytime you do anything for 277 million people, it ends up costing a lot.

So my guess is that it would cost a lot.

Mr. HORN. Now that we have locked in Presidents from putting their little hands in the Social Security trust funds, maybe they will have more money for administrative analysis. But right now, we have to appropriate that for administration? And you can't use what is in the trust fund? Am I right on that?

Mr. STRECKEWALD. Yes. If the new card were to go beyond the purposes of what the Social Security card is currently used for, we could not use the trust funds to pay for the cost.

Mr. HORN. Are there any other points you would like to make before we adjourn this hearing?

Dr. Twight.

Ms. TWIGHT. I wanted to comment on the point that was just made about private people's willingness to divulge their Social Security numbers for seemingly the most trivial of business transactions.

I recently had an experience at the Bon Marche in Boise, ID where I forgot my charge card and they just asked me for my Social Security number and I refused to give it.

But in any event, it seems that today so many people are willing to just divulge that Social Security number. My theory is that this gradual process by which the Social Security number has been used for everything—you have little kids growing up who have had the Social Security number since birth and so on—that people have become sort of desensitized to what that represents.

So I think that makes it even a larger problem than we might otherwise think.

Mr. HORN. Mr. Smith.

Mr. SMITH. I would like to defend people, if I may, with two examples.

I gave my Social Security number as a young person entering law school. Six years later, it shows up on the label of my alumni mailing to me so that it was open to the whole world. I didn't know the consequences of that when I provided my Social Security number. I provided it to an authority figure and figured that it was required.

I opened a bank account and was asked for a Social Security number because the Department of Treasury requires it. My bank was sold to another company that now wants to use it as the access code to get my account information over the telephone and use it as the last four digits of the PIN number.

I didn't provide it for that purpose. So I think people ought to be defended. They give out the Social Security number to authority figures without knowing the consequences of how it might be used later for secondary purposes.

Mr. HORN. I think you are absolutely right. I have had so many people tell me that. And I know in a couple of cases when I have said, "It's none of your damn business," they looked at me like I was a crook. So be it, and they didn't get the sale.

Mr. STRECKEWALD. Mr. Chairman, this bill could impact Social Security, even though we are actually exempted from some of the restrictions on it. We think it would interfere very much with our pledge to the American people to deliver services.

For years, our informal motto at SSA has been to pay the right check to the right person at the right time. This bill could interfere with all three of those.

Paying the right check, of course, is dependent upon knowing other sources of income. Without the data matches we have, either we would have to rely upon manual error prone processes or we would not be able to do them at all. So the right check would be in question.

Paying the right person is the same idea. The Social Security number is a unique identifier. We know which John Smith we are dealing with, so the use of Social Security numbers allows us to know that we get the right check to the right person.

And then the final piece, the right time, is referring to timely service so that people don't have to wait for their check. They don't have to wait for changes in the amount of their checks. Manual processes take a lot longer than automated computer matches, although we have no way of knowing right now exactly how much longer. It may create an additional burden on the American people to come and give us, on a regular basis, the information that we currently receive from these matches.

These are just some of our concerns about this bill.

Mr. HORN. Now, I am sure you are following the legislation we have already worked on in the last couple of months, and that is to relieve you of having to worry about this person having extra income to work and just wiping that out.

Will that help you in the sense that it doesn't matter who they are—and I think we have wasted a lot of administrative time, probably, in Social Security to try to get some poor soul that has $500 a month in a check and she is working in a local hardware store at minimum wage.

Won't that help you when we knock that out?

Mr. STRECKEWALD. I am not sure if I understand your question. Are you referring to——

Mr. HORN. We are talking about the employment thing I am talking about. I was curious how many thousands of people you have worrying about that, because we are going to relieve you of that.

Mr. STRECKEWALD. I see. You are talking about the elimination of the retirement earnings test.

Mr. HORN. That's right.

Mr. STRECKEWALD. That will definitely relieve people of reporting their earnings to us who are past the retirement age. You are right, there.

Mr. HORN. So we are looking at about 900,000 beneficiaries that might be affected by that. How many employees could you let go because they are no longer figuring that, or harassing people, or whatever?

Mr. STRECKEWALD. We haven't done that analysis yet, but I would be glad to submit something to you if we have anything.

Mr. HORN. I really would like to have that analysis and put that in the record, without objection, at this point because we are wondering at that. There are a lot of things you have to do and that is not going to be one of them anymore. I think everybody is going to be happier and they will have more money and it wasn't helping that much anyhow. But we have to argue and they go through our district offices because they have seen a deduction from their check and wonder what that is all about and they have to worry about writing out a check themselves when they don't have the money.

So I would hope that is relieving you of a lot of work.

Mr. STRECKEWALD. We will look into it.

Mr. HORN. Thank you very much. I would like the response put at this point in the record.

[The information referred to follows:]

IMPACT OF ELIMINATION OF RETIREMENT EARNINGS TEST

We would not reduce SSA's employment as a result of repeal of the retirement earnings test at normal retirement age. We had expected the level of effort devoted to this activity at SSA to fall off anyway, as the earnings threshold changed in the future. In order to implement the legislation in a timely manner and eliminate the retirement test for certain beneficiaries retroactive to January 2000, SSA had to defer other work to temporarily absorb the cost of the effort within appropriations enacted prior to the change in the law. For example, appointment calendars in the field offices backed up, resulting in claimants waiting longer to file their claims. In addition, we are seeing a greater increase than we expected in our claims workloads from people who wouldn't have filed if the test were still in effect.

As you know, the President's budget request for SSA over the past few years has been less than the Commissioner's budget, and Congress has reduced what the President requested. As a result, we have had to lower our performance targets. To the extent that we can eventually free up resources from the retirement earnings test, our plan would be to reinvest these resources in our public service and program integrity efforts.

Mr. HORN. Thank you. You have all been very good witnesses and we have learned a lot.

This is simply the first hearing to take a look at this situation. And I understand that the Ways and Means Committee that does have authorization on Social Security is also doing that. So maybe something good will come out of it.

We thank you for coming here and sharing.

And I will say to anyone else here that might want to file a statement, if you could file it in the next 2 weeks, we would be glad to put it in the record because I know a lot of groups at the State level, motor vehicles, the universities, and all the rest would like to get their views in on it, and we welcome them.

With that, we thank you and we thank the staff here: Russell George, the staff director and chief counsel; Heather Bailey to my left and your right, the professional staff member who put this one together; Bonnie Heald, director of communications is here; Bryan Sisk, clerk; Elizabeth Seong, intern; Michael Soon, intern; Trey Henderson, the counsel for the minority; along with Jean Gosa, the minority clerk. And we thank Mr. Mel Jones today for being the court reporter.

With that, we are adjourned. Thank you.

[Whereupon, at 3:41 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Statement of Mr. John Corder on the Freedom and Privacy Restoration Act (HR 220)
before the Subcommittee on Government Management, Information and Technology
of the Government Reform and Oversight Committee

05/18/2000

While I count it as a privilege and a duty to appear before this congressional subcommittee, I regret that the invitation notice was just too short for me to arrange my affairs to meet the hearing date.

However, I wish to offer my written testimony regarding the issue of the use of Social Security numbers as a standard identifier. During the last few years I have been trying to stop the State of Texas from mandating that I surrender my federal Social Security number to the different agencies within the state government such as the Plumbing Examining Board, the Railroad Commission, and the Liquid Petroleum Gas (LPG) division. I am also forced to surrender the Social Security number for purposes of auto registration, drivers' licenses, auto purchasing, and jury duty statement.

Furthermore, I am asked to surrender my federal Social Security number to many corporations, business, medical and doctor groups who have no reason to know my Social Security number. I am also asked to surrender my federal Social Security number to financial institutions not related to the Social Security Administration. When I ask why all these private companies need my number, all I am told is "it is a good thing for us to have, really."

It is not only my concern over my loss of privacy that leads me to support the Freedom and Privacy Restoration Act, it is also the fear of fraud by the criminal minded that could take my earthly means of supporting my precious family as well as the observation that federal government condones the growth of the use of the Social Security number as a universal identifier. I am a U.S. citizen in good standing, not a pervert or a deadbeat dad. I have never been arrested, yet the demand that I surrender my Social Security number has become rampant, intrusive and downright degrading -- causing me to loose faith in the protective service of law enforcement.

I am almost 72 years old and I fell set upon by the growing unwarranted contention that I should be treated as if I am guilty of wrongdoing -- even though I am not. It is because of my love for my country, and for my fellow citizens that I pray you will hear my plea and act to safeguard the pursuit of happiness and privacy of all Americans.

John H. Corder

John H. CORDER

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT FOR THE RECORD

JOHN T. SPOTILA

ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS

SUBMITTED TO

THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

18 MAY 2000

Mr. Chairman:

Thank you for inviting me to provide the Administration's views with respect to H.R. 220, the "The Freedom and Privacy Restoration Act." We appreciate the opportunity to share our thoughts on this legislation.

President Clinton and Vice President Gore strongly support efforts to safeguard individual privacy. As the President said on April 30, when announcing his new financial privacy proposal: "From our earliest days, part of what has made America unique has been our dedication to freedom, and the clear understanding that real freedom requires a certain space of personal privacy." Vice President Gore showed similar leadership in 1998 when he called for an Electronic Bill of Rights, emphasizing that we should all do our part to protect individual privacy, relying on private sector leadership where possible, on legislation when necessary, on responsible government handling of personal information, and on an informed public.

With this direction, the Clinton Administration is engaged in many initiatives to protect personal privacy. For example, the Department of Health and Human Services is working on significant rules to protect the privacy of patients' medical records. We have also supported enhanced legal protections for financial records, as announced by President Clinton only two weeks ago.

The Administration is committed to protecting the privacy of personal information held by the government. For example, this February 8, President Clinton signed an executive order that prohibits every federal department and agency from using genetic information in any hiring or promotion action. This order ensures that critical health information from genetic tests not be

used against federal employees. In addition, programs are underway to strengthen Government computer security to provide new privacy safeguards for personal information held by the Government.

As the Administrator of OIRA, I am especially pleased that OIRA in 1998 took on enhanced responsibility for coordinating privacy policy throughout the Administration. OIRA already had policy responsibility under the Privacy Act of 1974, which applies to federal government systems of records. Now it plays a central coordinating role for privacy policy more generally. Last year, OMB appointed its first Chief Counselor for Privacy to be the point person in this coordination effort. One of the first functions of the Chief Counselor was to ensure that all Federal agencies successfully posted clear privacy policies on their websites. We accomplished that goal in less than 4 months.

With respect to social security numbers, we agree that it is imperative for the government to handle such information with the utmost sensitivity. The Privacy Act of 1974 provides important protections against the misuse of an individual's personal information, including social security numbers.

- Under this Act, an agency may only disclose personal information with the individual's affirmative consent, subject to limited exceptions specified in the Act. Among these exceptions are disclosure: for intra-agency use, limited to people who need the information for the performance of their duties; pursuant to court order; and for statistical research purposes in form that does not identify the individual.
- The Act requires that individuals, at the time their information is collected, receive notice of the purposes for which the information will be used.
- The Act incorporates an important minimization principle – an agency may only maintain records about an individual that are relevant and necessary to accomplish a purpose required of the agency under a statute or executive order.
- Under the Act, an individual has a right to an accounting as to whom his or her records have been disclosed, when, and for what purpose.
- Under the Computer Matching and Privacy Protection Act of 1988 (CMPPA), an amendment to the Privacy Act, agencies must enter into an agreement with one another specifying how any computer data exchanged will be used and how it will be safeguarded. Under the CMPPA, individuals have the right to refute adverse information before having a benefit denied or terminated. The CMPPA also requires each agency to establish a Data Integrity Board to oversee matching activities.

The Privacy Act has special legal protections regarding the collection of social security numbers. It prohibits any federal, state, or local government agency from denying any individual a right, benefit, or privilege provided by law because of his or her refusal to disclose his or her social security number unless the disclosure is required by a Federal statute or covered by a grandfathering clause for certain pre-1975 activities. Moreover, any agency that requests such disclosure must inform the individual about whether the disclosure is mandatory or voluntary, by what authority, and what uses will be made of it.

The federal government does not sell social security numbers. It is sensitive to their confidentiality. Indeed, exemption 6 to the Freedom of Information Act (FOIA) protects social security numbers from disclosure when FOIA requests are made.

The Administration shares the Committee's concern that the improper disclosure of social security numbers can cause significant problems, including the risk of identity theft -- a serious crime of increasing incidence. One of our top priorities was the passage of strong identity theft legislation and we applaud Congress for enacting the Identity Theft Assumption and Deterrence Act of 1998. More recently, at the President's request, the Department of Treasury convened a National Summit on Identity Theft on March 15 and 16 of this year. This Summit brought together private sector companies, public interest groups, and government agencies to consider concrete initiatives to address this crime.

Our sense is that particular threats to privacy in this area are arising in the private sector. Commercial use of the social security number for identification purposes has become much more widespread. Social security numbers are used in processing applications to college, for commercial loans, and in countless other areas. This is an area that warrants more attention.

We agree that we must all work diligently to prevent the misuse of social security numbers in all areas, including government. We believe, however, that the approach taken in H.R. 220 could pose great risks to the government's ability to serve the American people. We understand that other agencies are submitting views to the Committee describing the adverse impact of this bill on their individual operations. We thought it important to emphasize the bill's potentially harmful effects in at least three crosscutting areas: (1) the ability to deliver benefits to the public; (2) the ability to use statistical programs to help direct federal funds; and (3) the ability to root out fraud and abuse through matching programs.

The government needs social security numbers to deliver benefits and services to American citizens. Prohibiting the use of a social security number and the inter-agency use of any identifier, as H.R. 220 proposes to do, would hamper our ability to serve the public. Thus, the Department of Veterans Affairs (VA) relies upon social security numbers to coordinate patient care across the various public and private entities that currently provide care to veterans. Consider also the approximately 2.6 million members of the armed forces who upon separation or discharge are eligible for benefits administered by the VA. VA and the Department of Defense (DOD) clearly must work together to ensure that the benefits paid by VA are paid to the correct former DOD armed service member in the correct amount. Social security numbers provide the identifying information that is necessary for such an assurance. Similarly, in disaster relief cases, the Federal Emergency Management Association and the Small Business Administration rely upon social security numbers to identify disaster victims and determine eligibility for needed housing, individual and family assistance, and disaster loans. Likewise, the unemployment compensation program depends upon the use of social security numbers to assure proper payments of benefits to jobless workers.

Under H.R. 220, these agencies would evidently need to use other agency-specific identifiers to ensure that the right beneficiary is paid the right amount. To authenticate the

identity of each individual before assigning such a number, the agency would presumably need to use address, telephone, mother's maiden name, and/or other verifying information. Such data can be unreliable for identification, however, because it is easy to falsify. To be more reliable, an agency might need to collect and compare more than one data element. Even so, the approach would be unreliable and would require additional time and resources. It may be that new technologies -- such as digital signatures as part of a public key infrastructure -- will eventually ease the government and private sector burden in authenticating the identity of individuals. Currently, agencies often lack this capability.

Social security numbers are also critical in carrying out many statistical programs that generate our Nation's key social and economic indicators. We have worked diligently to improve the efficiency and quality of our statistical system and to reduce the reporting burden on individuals and businesses. With your help, we have also endeavored to create and promote necessary safeguards to ensure confidentiality protection for information that is acquired exclusively for statistical purposes. Our ability to provide high quality statistics for national, state, and local decision making would be severely hampered by a prohibition on the linking of social security numbers to data for statistical purposes. The Census Bureau's Intercensal Population Estimates Program is one example of the losses in quality and efficiency that would result. The production of intercensal population estimates relies on the effective use of administrative records that contain social security numbers, and the ability to link those records across time and across various administrative sources of information. By law, the Census Bureau must produce annual estimates of the population and its characteristics. As with all other census information, these data cannot be released in individually identifiable form. These data are used extensively to allocate federal funds for such other important purposes as distributing state and local government services, planning utility services, and locating retail and manufacturing establishments. The inability to use social security numbers and the associated inability to link birth records, death records, and similar administrative data would require a total redesign of the Intercensal Population Estimates Program. Recent evaluations indicate that alternative methods would result in estimates that are less accurate and less timely than those currently produced. Thus, the quality of statistical data and the efficiency of producing this critical information would be seriously eroded.

Social security numbers are also a critical component in the federal government's efforts to eliminate fraud and abuse. For example, in one program, the Department of Education matches files of student loan defaulters via name and social security number with records held by HHS's Office of Child Support enforcement showing current home address, employment address and income. This match enables Education to contact the delinquent debtors through current address information, attempt to secure voluntary repayment and, as a last resort, garnish their wages to pay off the debt, provided their wages exceed a certain threshold. Our estimates predict that this program will save taxpayers approximately $1 billion over five years. In addition, the Department of Education and IRS currently have an income verification system for student loan borrowers who choose the Income Contingent Repayment (ICR) option. Under this option, the monthly payment amount is based on how much money the borrower earns after the borrower finishes his education. Education matches its data with IRS data -- again via name and social security number -- to determine how much a borrower's monthly payment should be. A third anti-fraud example is the use of the social security numbers to reduce improper payments in

employer-sponsored insurance. This match depends on social security numbers to link spouses together and to determine the beneficiaries' employers.

We believe that current law protects well against the misuse of social security numbers by government agencies. We also have concerns that H.R. 220 would significantly impair our ability to deliver benefits and services to the American people, to perform important statistical and research functions, and to eradicate fraud and error in federal payment programs. While we understand the good intentions of the cosponsors and share their strong commitment to the protection of individual privacy, we urge great caution with H.R. 220, lest it cause unintended adverse consequences that we would all regret.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance.

— FOR THE RECORD —

(Publication page references are not available for this document.)

Associated Press Newswires
Copyright 2000. The Associated Press. All Rights Reserved.

Thursday, May 11, 2000

House OKs change in law mandating ✦**Social Security numbers**✦ for licenses

By BOB ANEZ
Associated Press Writer

HELENA (AP) - The Senate was planning to act today on a bill immediately repealing a new law that requires ✦**Social Security numbers**✦ be provided by applicants seeking Montana hunting and fishing licenses.

The mandate, which took effect Jan. 1, was demanded of all the states by the federal ✦**government**✦ under threat that millions of dollars in welfare aid would be withheld from those who refused.

House Bill 9, which representatives sent to the Senate on a 79-21 vote Wednesday, gives those wanting a recreation license the option of providing some other identification number, such as the one on a

(Publication page references are not available for this document.)

driver's license. It also tells the state Department of Public Health and Human Services to ask the federal ✦**government**✦ to allow the change.

The law demanding the state collect ✦**Social Security numbers**✦ is part of a national effort to make it easier to track down parents who have failed to pay child support.

But the law has sparked opposition from people who consider the mandate an invasion of their privacy. One sportsmen's group has launched an initiative drive to repeal the law.

State officials have said abolishing the requirement would jeopardize $58 million a year in federal aid for welfare programs, including child support enforcement efforts.

Rep. Hal Harper, D-Helena, acknowledged his bill is risky, but said it is not as dangerous as a proposed initiative for the November ballot that would just repeal the law without an alternative.

He said federal officials have hinted that they might approve an exemption for the kind of idea contained in HB9. "We see a crack in the

(Publication page references are not available for this document.)

federal door at this point," Harper said.

He argued that his proposal is better than the possible initiative because HB9 would abolish the law immediately for those wanting to buy a license in advance of the fall hunting season. Waiting for the ballot measure, on the other hand, would leave the requirement on the books for another six months, he said.

Rep. Paul Clark, D-Trout Creek, said the last Legislature made the mistake of giving in to the federal ✦**government**✦ and enacting the mandate, so it falls to lawmakers to correct the error.

"There was no mistake," said Rep. Matt Brainard, R-Florence. "We knew what was going on. We were blackmailed by the federal ✦**government**✦."

Now, he said, citizens have discovered what the Legislature did and are demanding it be reversed.

Rep. Bob Clark, R-Ryegate, said the bill really does nothing to keep **←Social Security numbers→** out of the hands of more **←government→** officials. Using driver license numbers still would provide authorities with access

(Publication page references are not available for this document.)

to **←Social Security numbers→** that are necessary to get a driving license, he said.

Rep. Gary Beck, D-Deer Lodge, said those upset about the law already in place are overly concerned about **←government→** access to **←Social Security numbers→**.

"There's a certain amount of paranoia," he said. "I think we're making too much of a little issue."

Rep. Carolyn Squires, D-Missoula, became angry that opponents of the bill would rather endanger the state's access to federal money for welfare families and parents due child support.

"By not passing this legislation, you're damning them," she said. "We have a responsibility. We have $175 million out there in unpaid child support. Is that federal money? Hell no."

---- INDEX REFERENCES ----

KEY WORDS: AP STATE WIRES: MONTANA

(Publication page references are not available for this document.)

STORY ORIGIN: HELENA

NEWS CATEGORY: STATE AND REGIONAL

REGION: Montana; Western U.S.; United States; North America; United States - Montana; United States; North America; Pacific Rim (MT USW US NME USMT USA NAM PACRM)

Word Count: 543
5/11/00 APWIRES 02:05:00
END OF DOCUMENT

Copr. (C) West 2000 No Claim to Orig. U.S. Govt. Works

05/17/00 WED 17:54 FAX 202 514 9353 DOJ OLA 002

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 17, 2000

The Honorable Stephen Horn
Chairman
Subcommittee on Government Management,
Information and Technology
Committee on Government Reform
U.S. House of Representatives
Washington, D.C. 20530

Dear Chairman Horn:

This letter is in response to your request for the views of the Department of Justice on H.R. 220, the "Freedom and Privacy Restoration Act of 1999." We are providing our preliminary views on the bill, however, we require additional time to consider fully the impact of this legislation upon our work. It is our understanding that you also have requested the views of the Office of Management and Budget as well as those of several other agencies and that you will receive those views separately.

We recognize the need to protect the personal privacy of American citizens and we recognize that the misuse of Social Security numbers by private parties is a serious and growing problem. We appreciate H.R. 220's laudable goal of protecting personal privacy. However, our preliminary review raises numerous, serious concerns about H.R. 220. We look forward to working with members of Congress on other ways to prevent identity theft and abuses of personal privacy.

H.R. 220 would severely limit the lawful and necessary use of Social Security numbers by most government agencies. Several of the concerns we have about such a limitation are outlined below.

Law Enforcement Impeded

H.R. 220 could seriously harm law enforcement. Local, State and Federal law enforcement agencies routinely use Social Security numbers in a manner often critical to effective law enforcement. Currently, Social Security numbers are used for such functions as locating fugitives, identifying detainees, verifying prior criminal history records, locating outstanding warrants, and discovering fraudulent activity.

Social Security numbers are more reliable than other identifiers (such as name and date of birth) because they are verifiable and unique. Databases for other forms of identification are often inconsistent or inaccessible. For example, many localities' birth and name records are not computerized and some have been destroyed in floods or fires. Additionally, use of a unique identifier, such as a Social Security number, is essential because many individuals share common names, dates of birth and addresses.

Numerous Federal and State agencies responsible for administering "Federal benefits programs," as that term is used in the Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503, as amended, use Social Security numbers in computer matching programs with other agencies to verify the eligibility or continued eligibility of persons applying for or receiving these benefits. Reliance on less unique identifiers could lead to misidentification, resulting in the provision of benefits to large numbers of ineligible individuals; or, conversely, the erroneous denial or suspension of critical benefits (such as Medicaid, Food Stamps, AFDC, SSI, and other Social Security benefits) to eligible individuals. These are precisely the results that the Congress feared from the proliferation of computerized exchanges of data between agencies and sought to avoid by enacting the computer matching amendments to the Privacy Act. These amendments sought to ensure due process and the accuracy and integrity of data. A blanket prohibition on agencies' use of Social Security numbers for identification purposes could seriously undermine the goals of those amendments.

Separate law enforcement agencies routinely must share information from databases that use identifying numbers. Law enforcement agencies rely extensively on a wide range of databases that, in turn, rely heavily on Social Security numbers.

For example, Social Security numbers are used extensively by Criminal Justice Information Systems (CJIS), the Interstate Identification Index (III), and the Automated Fingerprint Identification System (AFIS) as well as numerous other record and identification systems used daily by the Federal Bureau of Investigation, other Federal law enforcement agencies, and thousands of State and local law enforcement agencies.

To the extent that driver identification numbers in some States historically have been identical to Social Security numbers; that social security numbers were provided and used in commercial, credit, financial, or other transactions; or that Social Security numbers have been used in the application for or receipt of Federal benefits, grants or contract payments; law enforcement agencies would have a similarly compelling need to use these numbers to identify individuals in the context of civil and criminal investigations and related proceedings that would predate the effective date of this legislation were it to be adopted. For example, in criminal health fraud investigations, the Department often relies upon the fact that Social Security numbers are the patient identification numbers for Medicare and Social Security. Similarly, Social Security numbers often provide critical assistance to law enforcement agencies in identifying accounts and account holders.

Our preliminary review of H.R. 220 also has revealed numerous other specific concerns about this legislation -- both substantive and technical -- that would adversely affect law enforcement. We would be happy to elaborate on those concerns after we have had sufficient time to review the legislation further.

Administrative Concerns

H.R. 220 would be burdensome to the Department in numerous other ways. For example, the Department's own personnel databases rely on Social Security numbers. We are continuing to review the full impact of H.R. 220 in this regard.

Constitutional Concerns

H.R. 220 would restrict the ability of State agencies to use Social Security numbers. Section 2 of the bill provides that no State "may use a social security account number . . . or any derivative of such a number as the means of identifying any

individual," and section 3 provides that no State "may request an individual to disclose his social security account number, on either a mandatory or voluntary basis."

We believe that some litigation risk exists that a litigant might challenge H.R. 220 as unconstitutional under the Tenth Amendment. The courts of appeals have disagreed over the limitations the Tenth Amendment places on Federal regulation of State activity. For example, the Fourth Circuit recently held that "Congress may regulate the conduct of the States only through laws of general applicability." Condon v. Reno, 155 F.3d 453, 462 (4th Cir. 1998) (holding that the Driver's Privacy Protection Act violates Tenth Amendment), reversed on other grounds, 120 S. Ct. 666 (2000). (In reversing, the Supreme Court did "not address the question whether general applicability is a constitutional requirement for federal regulation of the States." Id. at 672.); see also Pryor v. Reno, 171 F.3d 1281, 1286-87 (11th Cir. 1999), petition for cert. pending, No. 99-61. On the other hand, at least two circuit courts have disagreed with this view and have indicated that Congress may regulate State conduct, provided it does so in a nondiscriminatory manner, see Travis v. Reno, 163 F.3d 1000, 1006 (7th Cir. 1998), petition for cert. pending, No. 98-1818, and does not "commandeer the state legislative process" or "conscript state officials to enforce federal law," Oklahoma v. United States, 161 F.3d 1266, 1272 (10th Cir. 1998), petition for cert. pending, No. 98-1760. The United States has taken the position that "[n]o constitutional rule requires Congress to regulate state activity in or affecting commerce only through statutes that also regulate similar private activity." Brief for the Petitioners at 18, Reno v. Condon, No. 98-1464 (1999). Thus, while we believe that H.R. 220 is constitutional, we believe that it poses a litigation risk.

Again, although we have numerous serious concerns regarding this legislation, we look forward to working with you on other ways to protect the privacy of Americans and deter the improper use of Social Security numbers.

Thank you for the opportunity to comment on this legislation. If we may be of additional assistance, we trust that you will not hesitate to call upon us. The Office of Management and Budget has advised us that, from the standpoint of

the Administration's program, there is no objection to the submission of this letter.

Sincerely,

Robert Raben
Assistant Attorney General

IDENTICAL LETTER SENT TO THE HONORABLE JIM TURNER, RANKING MINORITY MEMBER

6/25/2000
In our hearing with IRS Com. Rossotti, I raised the problem Kenny Knapp. Did the Com. ever respond? Did I ask? Please check the transcript.
D

2-17-00

Dan Burton
Government Reform & Oversight Committee
2185 Rayburn House Office Building
Washington, DC 20515-1406

Certified Receipt # Z 474 967 495

Subject: "Illegal Deficiency Notice"

Dear Mr. Burton,

As a member of the Oversight Committee I feel compelled to forward the enclosed letter from District Director - Deborah Decker and my reply.

My reply is rather self-explanatory. It is my sincere wish to witness the eradication of these illegal and extortionary tactics perpetrated by the IRS.

I believe with the help of other members of congress you can lead the battle against these egregious acts.

Sincerely, I Remain,

Kenny Knapp

Kenny Knapp
P.O. box 775092
Steamboat Springs, CO 80477

P 911 057 207

EXM00

Department of Treasury
Internal Revenue Service
OGDEN, UT 84201

Letter Number: 3219(SC/CG)
Letter Date: FEBRUARY 11, 2000

Taxpayer Identification Number:
526-08-1492

Tax Form: 1040

Tax Year Ended and Deficiency
DECEMBER 31, 1998 $4,364.3

Contact Person:
CORRESPONDENCE EXAM TECHNICIAN

Contact Telephone Number:
(801) 620-7474
(NOT A TOLL FREE NUMBER)
Hours to Call:
7:00 AM TO 7:00 PM MON-FRI

Last Date to Petition Tax Court:
MAY 11, 2000

KENNY KNAPP
PO BOX 775092
STEAMBOAT SPRINGS, CO 80477-5092927

Penalties/Additions to Tax
IRC Sections 6662(a) & 6662(b)(1) $872.86

Dear Taxpayer:

We have determined that there is a deficiency (increase) in your income tax as shown above. This letter is your NOTICE OF DEFICIENCY, as required by law. The enclosed statement shows how we figured the deficiency.

If you want to contest this determination in court before making any payment, you have until the Last Date to Petition Tax Court (90 days from the date of this letter or 150 days if the letter is addressed to you outside the United States) to file a petition with the United States Tax Court for a redetermination of the amount of your tax. You can get a petition form and the rules for filing a petition from the Tax Court. You should file the petition with the **United States Tax Court, 400 Second Street NW, Washington D.C. 20217.** Attach a copy of this letter to the petition.

The time in which you must file a petition with the court (90 days or 150 days as the case may be is fixed by law and the Court cannot consider your case if the petition is filed late. As required by law, separate notices are sent to spouses. If this letter is addressed to both a husband and wife, and both want to petition the Tax Court, both must sign the petition or each must file a separate, signed petition.

The Tax Court has a simplified procedure for small tax cases when the amount in dispute is $50,000 or less for any one tax year. You can also get information about this procedure, as well as a petition form you can use, by writing to the Clerk of the United States Tax Court at 400 Second Street, NW, Washington, D.C. 20217. You should write promptly if you intend to file a petition with the Tax Court.

If you decide *not* to file a petition with the Tax Court, please sign and return the enclosed waiver form to us. This will permit us to assess the deficiency quickly and will limit the accumulation of interest. We've enclosed an envelope you can use. If you decide not to sign and return the waiver and you do not petition the Tax Court, the law requires us to assess and

If you have questions about this letter, you may call the Contact Person whose name and telephone number are shown in the heading of this letter. If this number is outside your local calling area, there will be a long distance charge to you. If you prefer, you can call the Internal Revenue Service (IRS) telephone number in your local directory. An IRS employee there may be able to help you, but the office at the address shown on this letter is most familiar with your case.

When you send information we requested or if you write to us about this letter, please provide a telephone number and the best time to call you if we need more information. Please attach this letter to your correspondence to help us identify your case. Keep the copy for your records.

The person whose name and telephone number are shown in the heading of this letter can access your tax information and help get you answers. You also have the right to contact the Taxpayer Advocate. You can call 1-800-829-1040 and ask for Taxpayer Advocate Assistance. Or you can contact the Taxpayer Advocate for the IRS Office that issued this Notice of Deficiency by calling (801) 620-7168 or writing to:

OGDEN SERVICE CENTER
TAXPAYER ADVOCATE
P.O. BOX 9941, STOP 1005
OGDEN, UT 84409

Taxpayer Advocate assistance is not a substitute for established IRS procedures such as the formal appeals process. The Taxpayer Advocate is not able to reverse legally correct tax determinations, nor extend the time fixed by law that you have to file a petition in the United States Tax Court. The Taxpayer Advocate can, however, see that a tax matter that may not have been resolved through normal channels gets prompt and proper handling.

Thank you for your cooperation.

Sincerely yours,

Commissioner
By

Deborah S. Decker

DEBORAH S. DECKER
DIRECTOR, OGDEN
CUSTOMER SERVICE CENTER

Enclosures:
Copy of this letter
Waiver
Envelope

February 17th, 2000

Director-IRS Service Center
Internal Revenue Service
Ogden, UT 84201

Certified Receipt # Z 474 967 488

Subject: Deficiency Notice dated 2-11-00

Attention: Deborah S. Decker

According to your **"Deficiency Notice"** of the above date (cover sheet attached), there is an alleged deficiency with respect to my 1998 income tax of $4 364.30, and if I wanted to "contest this deficiency before making payment," I must "file a petition with the United States Tax Court." Before I file, pay, or do anything with respect to your "Notice" I must first establish whether it was sent pursuant to law, whether it has the "force and effect of law," and whether you had any authority to send me the Notice in the first place.

I have attached to this letter an excerpt from the Supreme Court decision **FEDERAL CROP INSURANCE CORP v A.A. MERRILL, 332 U.S. 380** note that the Court held in that case that:

Anyone entering into an arrangement with the government takes a risk of having accurately ascertained that he who purports to act for the government stays within the bounds of his authority, even though the agent himself may be unaware of the limitations upon his authority. (emphasis added)

Note that the Supreme Court in this decision warns the public that those who pay attention to what federal employees say **"take the risk"** that such employees may not be acting "within the bounds of (their) authority" and that such employees may even be **"unaware of the limitations of (their) authority."**

Well I am <u>not</u> **PREPARED TO TAKE THAT "RISK."**

Let me further point out that IR Code Sections 6001 ad 6011 (as identified in the 1040 Privacy Act) notifies me that I need only "comply with regulations." <u>**Nothing in the Privacy Act notice or in the above statutes informs me that I have "comply" with, or pay attention to, letters and/or alleged "determinations" ent to me by various and sundry employees of the IRS.**</u>

Please note that Section 6212 states that "**If the Secretary determines** that there is a deficiency in respect of any tax....**he is authorized to send notice of such deficiency etc., etc.**" However, the "Notice" I received was not sent by the Secretary, but by Deborah S. Decker who is identified as being the Director of the IRS Service Center in Ogden, UT., and I have no way of knowing whether she has been delegated by the Secretary to send such notices on the Secretary's behalf. So before I do anything at all with respect to your "Notice," I would have to see a Delegation Order from the Secretary of the Treasury delegating Deborah Decker the authority to send Deficiency Notices. !?

In addition, I would also like you to send me (or identify for me) the **legislative regulations** that **you claim implement Code Sections 6212 and 6213.**

I have also attached an excerpt from the IRS Procedures Manual (MT 1218-196, at page P-6-40) which points out that the IRS is required to "make available to all taxpayers comprehensive, accurate, and timely information on the requirements of tax law and regulations." So, pursuant to this provision from your Procedures Manual, I am asking that you **identify ("make available") for me the legislative regulations that you claim implement both Code Sections 6212 and 6213** - since I could not locate them.

Without you furnishing me with these documents and information, I will be unable to "ascertain" (pursuant to the Federal Crop decision cited above) whether the individual who sent me the Deficiency Notice was authorized to do so, and whether I am legally required to take any notice of it. I am obviously unwilling to "take the risk" referred to by the Supreme Court in the above cited case.

I have receipts for several certified letters sent to the Secretary of Treasury, IRS Commissioner Charles Rossetti, IRS District Director Walter Hutton, and to the Ogden, UT IRS Center asking for a meeting where the statute and implementing regulations making me liable for any "income" tax and the Delegation of Authority from the Secretary delegating authority to the various IRS agents to proceed as they have will be provided. I have never received a reply from anyone addressing my concerns which in itself is a direct violation of the Administrative Procedures Act. I am being denied due process. Deborah Decker and Dennis Paiz, you have completely ignored your own mission statement, the Taxpayer's Bill of Rights and several regulations violating the laws of this country.

I cannot and will not let these egregious violations go unanswered.

And let me further add that if the IRS attempts to assess and collect the alleged Deficiency by distraint without responding to my above requests, I will sue the government pursuant to Code Section 7433 because the IRS will be **"recklessly and intentionally disregarding"** the statutes mentioned above together with their implementing regulations (or lack thereof) along with a number of other statutes that I need not list and/or identify here.

Constitutionally yours,

Kenny Knapp

Enclosures/ Federal Crop Insurance Decision

CC by Registered Mail to:

Secretary of Treasury
Charles O. Rossotti, Commissioner of Internal Revenue
Senator Charles Roth - Senate Finance Committee - Tax and IRS Oversight Sub-Committee
Bill Archer - Chairman - Congressional committee - Ways and Means Sub-Committee

FEDERAL CROP INSURANCE CORPORATION

v.

A. A. MERRILL and N. D. Merrill, Co-partners, Doing Business under the Firm Name and Style of Merrill Bros.

(332 US 380–388.)

HEADNOTES

Classified to U.S. Supreme Court Digest, Annotated

United States, § 69 — contracts — liability — tests.

1. The fact that the government has taken over a business or is engaging in competition with private ventures does not subject it to the same tests of liability as in the case of private individuals.

Insurance, § 20 — by governmental agency — liability for acts of agents.

2. The rules of law whereby private insurance companies are rendered liable for the acts of their agents are not bodily applicable to the Federal Crop Insurance Corporation unless Congress has so provided.

[*See annotation reference*, 1.]

Corporations, § 233; United States, § 25 — governmental agencies.

3. The government may carry on its operations through convenient executive agencies or through corporate forms especially created for defined ends.

United States, § 87 — powers of agent — duty to ascertain.

4. Anyone entering into an arrangement with the government takes the risk of having accurately ascertained that he who purports to act for the government stays within the bounds of his authority, even though the agent himself may be unaware of the limitations upon his authority.

Insurance, § 164 — estoppel by agent's knowledge of facts — Federal Crop Insurance Corporation.

5. The Federal Crop Insurance Corporation is not bound by assurance given to a farmer by its local agents that his crop was insurable, where a valid regulation published in the Federal Register but not in fact known to the farmer or to the local agents precluded coverage. [Four Justices dissented.]

[*See annotation references*, 1 and 2.]

EXHIBIT 1

RG - for hearing record

Marshall E. Whitenton
Vice President
Resources, Environment, and Regulation

June 20, 2000

The Honorable Steve Horn
Chairman
Subcommittee on Government Management, Information and Technology
House Committee on Government Reform
U.S. House of Representatives
B-373 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

The National Association of Manufacturers (NAM) welcomes the hearing on H.R. 4246, the Cyber Security Information Act. The NAM – 18 million people who make things in America – is the nation's largest and oldest multi-industry trade association. The NAM represents 14,000 member companies (including 10,000 small and mid-sized companies) and 350 member associations serving manufacturers and employees in every industrial sector and all 50 states.

The NAM affirms the findings and premises behind this bill. One cannot responsibly disregard the possibility that the same hostile powers or groups that would blow up a U.S. aircraft, or attack a U.S. embassy or federal office building, would also seek to inflict damage by a computer-related attack. The NAM has commended President Clinton for his critical infrastructure protection initiative.

Already, Congress has decided that protection against terrorism requires an adjustment to the Freedom of Information Act (FOIA). In last year's Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA), Congress removed parts of certain reports mandated under Section 112(r) of the Clean Air Act from FOIA release. Specifically, the hypothetical off-site consequence analyses submitted to the Environmental Protection Agency (EPA) by thousands of chemical-producing and -using facilities – or "worst case scenarios" – will now be available in limited format and numbers. The intent is to prevent terrorists from reconstructing a "hit list" of facilitates whose attack would result in the greatest number of casualties (see the joint proposed rule from the EPA and the Department of Justice, 65 *Federal Register* 24834, April 27, 2000).

The June 22 hearing is therefore very timely. Even with last year's welcome legislation – passed by Congress just as the deadline for response to FOIA requests immediately submitted to EPA had arrived – the FOIA status quo cannot be called satisfactory. Agencies have discretion to withhold cyberthreat information voluntarily submitted by industry but are not required to do so. Strong guidance to agencies from the Department of Justice would certainly help. A statutory enactment would be even more forceful.

1331 Pennsylvania Avenue, NW • Washington, DC 20004-1790 • (202) 637-3157 • Fax (202) 637-3182 • mwhitenton@nam.org • www.nam.org

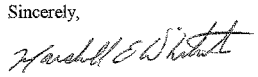
The NAM appreciates and values the FOIA. Indeed, the NAM files FOIA requests itself from time to time and agrees that this legislation should not narrow the FOIA beyond the minimum amount necessary to accomplish the key objectives of the critical infrastructure initiative. However, in our view, companies cannot be expected to reveal their vulnerabilities or losses without the greatest confidence that the information will not leave the hands of the government agency or agencies involved. That confidence simply does not now exist.

H.R. 4246 offers one approach to amending the FOIA. The NAM can support it as introduced. At the same time, the NAM is willing to consider supporting other drafting approaches. The drafting challenge is to create the conditions of confidence for industry, while reassuring groups traditionally supportive of the FOIA that the new provisions will not be misused.

The NAM also supports the antitrust exemption provided by H.R.4246. Just as with the successful National Security Telecommunications Advisory Committee, now 18 years old, many companies will have to work together. Removing the cloud of uncertainty about possible antitrust liability will reduce legal costs, improve information flow and promote the goals of the critical infrastructure protection initiative.

The NAM is an active partner in the Critical Infrastructure Partnership and looks forward to working with the subcommittee as the legislation progresses. For further information, you may contact David Peyton, director, technology policy, (202) 637-3147, dpeyton@nam.org; Larry Fineran, assistant vice president, resources, environment and regulation, (202) 637-3174, lfineran@nam.org; or myself.

Sincerely,



Marshall E. Whitenton
Vice President
Resources, Environment and Regulation

cc: The Honorable Thomas Davis, III
The Honorable James Moran

U.S. GENERAL SERVICES ADMINISTRATION
Office of Congressional and Intergovernmental Affairs

May 18, 2000

The Honorable Stephen Horn
Chairman
Subcommittee on Government Management,
Information, and Technology
Committee on Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

This is in response to your letter of May 5, 2000, to David Barram, Administrator of General Services requesting the views of the General Services Administration (GSA) on H.R. 220, the "Freedom and Privacy Restoration Act." GSA has reviewed the legislation and would like to offer the following comments.

After reviewing the above-referenced bill, we raise a concern under **Section 2. Restrictions on the Use of the Social Security Account Number Section C(i)**, which states:

> . . . [N]o agency or instrumentality of the Federal Government . . . may use a social security account number issued under this subsection or any derivative of such a number as the means of identifying any individual.

In the arena of Federal government contracts, a sole proprietorship "small business" is identified by a Taxpayer Identification Number (TIN Number) for tax and other reporting purposes. Often, a TIN Number of a small business is the individual business owner's personal social security number as well.

GSA is concerned that the current section 2 language might cover social security numbers being used as TINS, which would have a significant negative impact on many of our programs. For example, that section would make it very difficult to identify and report procurement information with small businesses including vendor payments and the number of small businesses contracting with Federal agencies.

1800 F Street, NW, Washington, DC 20405-0002

Federal Recycling Program Printed on Recycled Paper

Therefore, as a procurement policy agency, the GSA would urge that the definition of "social security number" exclude any individual's "social security number" "used for purposes other than as a means of identifying any individual."

Our Office of Inspector General (OIG), believes that the bill's potential impact on Federal agencies' operations and programs is far-reaching. However, they have confined their comments to potential impacts on their organization. As a general matter, they believe the bill may impede certain law enforcement tools, such as criminal records checks, that we conduct in the course of performing our mission. They believe generally that strict enforcement of existing privacy statutes more than adequately protects against misuse or access to personal information.

Their main concern is that the bill appears to prevent Federal agencies from using identifiers -- like social security numbers -- in investigations or oversight activities relating to transactions where the government is not a party. As a law enforcement office that conducts a range of criminal investigations, their Office of Investigations routinely runs criminal records checks on individuals or companies that are the subjects of investigation. These checks provide them with information ranging from whether the subject is armed and dangerous to prior arrest information. In order to retrieve this information, they rely on social security numbers, as well as other identifiers including names or dates of birth. Prohibiting them from using social security numbers, or other identifying numbers, would impede their -- and other law enforcement entities' -- ability to effectively use these resources. Practically speaking, multiple people may share the same name and date of birth; social security numbers provide one of the most reliable ways to positively identify an investigative subject.

The Office of Management and Budget has advised that there is no objection to the submission of these comments from the standpoint of the Administration's program.

Sincerely,

William R. Ratchford
Associate Administrator

Federal Recycling Program Printed on Recycled Paper

United States General Accounting Office
Washington, DC 20548

Health, Education, and
Human Services Division

B-286077

August 21, 2000

The Honorable Steve Horn
Chairman, Subcommittee on Government Management, Information, and Technology
Committee on Government Reform
House of Representatives

Subject: Responses to Questions From May 18th Hearing on Uses of Social Security Numbers

Dear Mr. Chairman:

I would like to thank you for the opportunity to testify at the May 18, 2000, hearing on the uses of Social Security Numbers (SSN). At that hearing, I agreed to get back to you on two questions, and today I am providing you with the information we were able to obtain.

First, you asked what problems are caused when necessary SSNs are not included on tax forms submitted to the Internal Revenue Service (IRS). When this occurs, IRS cannot link the taxpayer's information to other relevant past or future records. Basically, if IRS receives a tax return that does not contain the SSN of the primary taxpayer (the one filing the return),[1] the return is not to be processed until an SSN is obtained, generally by corresponding with the taxpayer. Also, if the return does not contain an SSN for a dependent child or a child for whom the taxpayer is claiming the Earned Income Tax Credit, the return is processed, but the taxpayer is not to be allowed a dependent exemption or any deduction or credit associated with the dependent, such as the credit for child and dependent care expenses and the child tax credit. If taxpayers later provide the missing SSNs, they are to be allowed the dependent exemption and any credit associated with the SSN. When SSNs are missing from information returns, such as forms 1099 for interest income and dividends, these are sent back to the payer.

Second, you asked what actions federal agencies are taking in the area of using biometrics to identify individuals. Biometric recognition provides automated methods of identifying a person on the basis of a physiological or behavioral characteristic. Various human characteristics are used for biometric recognition, including

[1]On a joint return the primary taxpayer is the one whose name is first on the return.

fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. Biometric recognition can be used for both identification and verification. For instance, biometric recognition can be used to identify an individual by searching a database consisting of an entire enrolled population for a match. A biometric system can also be used to verify, or authenticate, a person's claimed identity by determining whether it matches his or her previously enrolled pattern. Possible uses also include control of physical access to restricted areas, network security, and computer security. We found a number of examples of biometrics in use or under consideration in the federal government.

- The Immigration and Naturalization Service (INS) is using biometric recognition to provide prompt admission for authorized travelers to the United States by allowing them to bypass the personal interview/inspection part of the entry process. Specifically, INS uses hand geometry to verify the identity of the traveler at an automated inspection station. Travelers arriving at a port of entry proceed to an INS Passenger Accelerated Service System (INSPASS) kiosk, where they insert a card in a machine similar to an automated bank teller machine. They respond to messages (such as "enter flight number") on the touch-screen display and place their hand in a hand geometry reader.[2] The kiosk software automatically compares the live scan of the traveler's hand geometry to the image captured at enrollment. If the traveler's identity is validated, he or she can proceed. If not, the traveler is instructed to see an Immigration Inspector. The INSPASS system has been installed at international airports at Los Angeles, Miami, Newark, New York (John F. Kennedy Airport), and San Francisco.

- The INS also uses Port Passenger Accelerated Service System (PORTPASS) to monitor people in vehicles at borders through voice recognition. This system is currently being used at the U.S.-Canadian vehicle border crossing, and INS plans to use the same system at the U.S.-Mexican border crossing.

- The Federal Bureau of Prisons is using hand geometry units to monitor the movements of prisoners, staff, and visitors within certain federal prisons. Visitors must enroll upon entry and are given a magnetic stripe card containing information that points to their identifying information in a central database. They must carry this card with them at all times. Staff and inmates must also enroll in the system. Prison staff are enrolled to reduce the possibility of mistakenly identifying them as an inmate or for positive identification in the event of a disturbance. Prisoners are enrolled for access control to places such as the cafeteria, recreation lounges, and the hospital.

[2]INSPASS is used for citizens of 23 countries that are enrolled in the U.S. visa waiver program and visit the United States on business at least three times a year. In addition, diplomats, representatives to international organizations, and airline crews from the visa waiver program may voluntarily enroll in the INSPASS program.

- Federal law enforcement agencies such as the Federal Bureau of Investigation use an automated fingerprint identification system to more quickly search a database and match fingerprints of suspected criminals.

- Several federal agencies, including the Defense Advanced Research Projects Agency, Drug Enforcement Agency, Department of Defense, Department of Energy, Department of State, the Federal Bureau of Investigation, and the U.S. Mint, have acquired biometric devices for access control applications. The Department of Defense is researching biometrics as a means for enhancing computer network security. The Department of State is analyzing how biometrics might enable it to process passports and visas more efficiently.

- The General Services Administration (GSA) is working on implementing a system of "smart cards" for federal agencies.[3] In May 2000 GSA awarded governmentwide Smart Access Common ID contracts to five prime companies. These contracts, which are worth a maximum of $1.5 billion over a 10-year period, will provide the federal government with a wide range of smart card applications, including visual identification and authentication, and logical and physical access control. These applications may be supported by a variety of technologies, including biometrics, digital signatures, digitized photographs, and magnetic stripes. Currently, GSA is working with its five prime contractors to develop the smart card. According to GSA, various agencies have already expressed an interest in participating in the Smart Access Common ID contracts for both physical access to buildings and logical access to computer systems. These agencies include the Department of Defense, Department of State, Department of Justice, and Department of Veterans Affairs.

State and local governments have also implemented biometric technologies, primarily for use in the process of determining eligibility for public assistance benefits or entitlements. Pilot programs in several states report that they have experienced significant savings by requiring biometric verification for individuals applying for public benefits. For example, Los Angeles County in California implemented the Automated Fingerprint Image Reporting and Match (AFIRM) system to check the fingerprints of new welfare applicants against a database of prior claimants. The purpose of the system is to detect and deter fraudulent and duplicate benefit claims. California estimates that finger-imaging of welfare clients in just seven counties has saved about $86 million in the first 2 years of operation. The states of New York and Connecticut have implemented similar systems, reporting savings of $396 million and $15 million, respectively, in their first few years of operation. Moreover, such systems can be cost effective. For example, the state of Connecticut reports that it originally paid $5.2 million for its biometric identification systems and saved $9 million in the first year of operation. Eight states—Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York, and Texas—currently have biometric

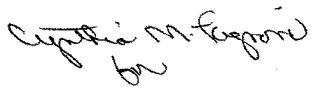
[3]The development of smart cards for federal employees originated in recommendations from the National Performance Review and the Government Information Technology Services Board.

identification systems in place or in pilot mode. Other states considering such systems include Florida, Pennsylvania, and North Carolina.

I hope this information is helpful. We will make copies of this letter available to those who request it.

If you or your staff have any questions, please call me or Kay Brown, Assistant Director, at (202) 512-7215. Other staff who assisted in gathering this information include David Attianese, Yvette Banks, Ralph Block, and Jeremy Cox.

Sincerely yours,



Barbara D. Bovbjerg
Associate Director, Education,
Workforce, and Income Security Issues

(207106)

RALPH REGULA, OHIO
JERRY LEWIS, CALIFORNIA
JOHN EDWARD PORTER, ILLINOIS
HAROLD ROGERS, KENTUCKY
JOE SKEEN, NEW MEXICO
FRANK R. WOLF, VIRGINIA
TOM DELAY, TEXAS
JIM KOLBE, ARIZONA
RON PACKARD, CALIFORNIA
SONNY CALLAHAN, ALABAMA
JAMES T. WALSH, NEW YORK
CHARLES H. TAYLOR, NORTH CAROLINA
DAVID L. HOBSON, OHIO
ERNEST J. ISTOOK, JR., OKLAHOMA
HENRY BONILLA, TEXAS
JOE KNOLLENBERG, MICHIGAN
DAN MILLER, FLORIDA
JAY DICKEY, ARKANSAS
JACK KINGSTON, GEORGIA
RODNEY P. FRELINGHUYSEN, NEW JERSEY
ROGER F. WICKER, MISSISSIPPI
GEORGE R. NETHERCUTT, JR., WASHINGTON
RANDY "DUKE" CUNNINGHAM, CALIFORNIA
TODD TIAHRT, KANSAS
ZACH WAMP, TENNESSEE
TOM LATHAM, IOWA
ANNE M. NORTHUP, KENTUCKY
ROBERT B. ADERHOLT, ALABAMA
JO ANN EMERSON, MISSOURI
JOHN E. SUNUNU, NEW HAMPSHIRE
KAY GRANGER, TEXAS
JOHN E. PETERSON, PENNSYLVANIA
VIRGIL H. GOODE, JR., VIRGINIA

Congress of the United States
House of Representatives
Committee on Appropriations
Washington, DC 20515–6015

DAVID R. OBEY, WISCONSIN
JOHN P. MURTHA, PENNSYLVANIA
NORMAN D. DICKS, WASHINGTON
MARTIN OLAV SABO, MINNESOTA
JULIAN C. DIXON, CALIFORNIA
STENY H. HOYER, MARYLAND
ALAN B. MOLLOHAN, WEST VIRGINIA
MARCY KAPTUR, OHIO
NANCY PELOSI, CALIFORNIA
PETER J. VISCLOSKY, INDIANA
NITA M. LOWEY, NEW YORK
JOSE E. SERRANO, NEW YORK
ROSA L. DELAURO, CONNECTICUT
JAMES P. MORAN, VIRGINIA
JOHN W. OLVER, MASSACHUSETTS
ED PASTOR, ARIZONA
CARRIE P. MEEK, FLORIDA
DAVID E. PRICE, NORTH CAROLINA
MICHAEL P. FORBES, NEW YORK
CHET EDWARDS, TEXAS
ROBERT E. "BUD" CRAMER, JR., ALABAMA
MAURICE D. HINCHEY, NEW YORK
LUCILLE ROYBAL-ALLARD, CALIFORNIA
SAM FARR, CALIFORNIA
JESSE L. JACKSON, JR., ILLINOIS
CAROLYN C. KILPATRICK, MICHIGAN
ALLEN BOYD, FLORIDA

CLERK AND STAFF DIRECTOR
JAMES W. DYER
TELEPHONE
(202) 225-2771

AUG 21 2000

David M. Walker
Comptroller General, U.S. General Accounting Office
441 G Street NW
Washington, DC 20548

00-1483

Dear Mr. Walker,

I request that the General Accounting Office investigate the Pentagon's recent decision to provide military hardware and services for a display near the Republican National Convention in Philadelphia. I request GAO to determine the following:

The legal basis for providing military equipment and services at taxpayer expense for functions that directly or indirectly support a political convention;

Whether the Department of Defense fully complied with existing law Congressional intent, and Defense regulations by providing such a display at taxpayer expense;

Whether the display was conducted in a manner to fully comply with law and Defense regulations;

Whether the display was used in any manner to support political or fundraising events; and

The total cost of the display, to include all indirect costs such as manpower.

Please provide a letter report to the Appropriations Committee, minority by September 15, 2000. David Kilian of the minority staff (225-3481) is my point of contact for this request. Thank you for your assistance.

Sincerely,

David Obey

New York Times
July 28, 2000

Pentagon Taking Opportunity For Show

By Steven Lee Myers

WASHINGTON, July 27 -- Despite a policy prohibiting military involvement in partisan politics, congressmen and guests at the Republican National Convention will have an exclusive viewing of some of the Pentagon's latest hardware, including an aircraft that the expected Republican vice-presidential nominee, Dick Cheney, tried to kill when he was secretary of defense.

Seizing what a spokesman today called "a convenient opportunity" to display some of its latest equipment, the Pentagon asked the armed services to ship -- at taxpayer expense -- weapons and other equipment to the former Philadelphia Naval Shipyard for what amounts to a three-day military trade show, beginning Saturday.

Secretary of Defense William S. Cohen, the only Republican in President Clinton's cabinet, approved the display after receiving a written request earlier this month from Representative Curt Weldon, a Republican from suburban Philadelphia and senior member of the House Armed Services Committee.

Mr. Cohen did so, officials said, only after the Pentagon was assured that the hardware -- and more than 150 service members accompanying it -- would not be used for any political activities.

To emphasize the point, the assistant secretary of defense for legislative affairs, John K. Veroneau, sent Mr. Weldon a letter outlining certain conditions: in short, no photo opportunities.

Even so, the display will be a centerpiece of a series of events organized by Mr. Weldon for about 100 Republican colleagues and their families, who will be staying in old Navy billets at the shipyard during the convention at the First Union Center, less than a mile away. Included in the festivities, closed to the public, will be a "block party" fund-raiser by Mr. Weldon on Monday.

"This whole thing is awkward," said Charles Lewis, executive director of the Center for Public Integrity, a nonprofit group in Washington. "All this sexy, multibillion-dollar hardware there to impress delegates is very smarmy and probably inappropriate. If there isn't a rule against this, it seems to me there ought to be."

The Pentagon's role has even raised hackles among some military officers, who complained that, at best, it blurs the definition of what constitutes political activity. "To say this is not a partisan event is borderline absurd," one officer said.

Others at the Pentagon complained that the cost would have to come out of their own budgets, at a time they face spot shortages of money for readiness.

Despite those misgivings, some of the services now appear to regard the display as a chance to do a little lobbying of their own. "There's not a lot of enthusiasm for this," another official said, "but if they're ordered to do it, they want to look good."

Among the aircraft to be displayed is the V-22 Osprey, which has crashed three times in the past decade. It is a hybrid with rotors that swivel so it can take off like a helicopter but cruise like a turboprop commuter plane. The Osprey has been beset by controversy over cost and mission as well as safety, and Mr. Cheney waged a long and unsuccessful battle against it when he was in the Bush administration.

In addition to the V-22, the Marines are sending an amphibious vehicle and equipment for its chemical- and biological-attack response teams. The Air Force plans to include an unmanned surveillance aircraft called the Predator, as well as missiles and bombs and story boards promoting its newest fighter, the

F-22.

The Army, not to be outdone, has mobilized a virtual armory of equipment, including an Apache attack helicopter, its own unmanned aircraft and its troubled theater missile defense system.

The Pennsylvania National Guard is contributing an M1-A1 tank, an armored personnel carrier and two more helicopters.

By contrast, the Navy is sending only an aging Sea Sprite helicopter from a nearby reserve unit, two surveillance vehicles and a small riverine boat.

Pentagon officials said today that it was too soon to put a cost on moving all the equipment to Philadelphia, though the Air Force estimated that its share would be at least $100,000.

The Pentagon's spokesman, Kenneth H. Bacon, spent much of a news conference today defending the display. Mr. Bacon said that the events at the shipyard were an opportunity to provide what amounted to a briefing to lawmakers -- without mentioning lobbyists and other influential Republicans who might happen by -- but maintained that the display was not itself partisan.

"It is something that's contemporaneous with the Republican National Convention," he said. "It's not adjacent -- it's not right on the grounds where the convention is being held. It's nearby, but not on the grounds."

Mr. Bacon also noted that Representative Robert A. Brady, a Democrat whose district includes the shipyard, supported the request, though he did not sign Mr. Weldon's request to Secretary Cohen.

Mr. Weldon's spokesman, Pete Peterson, said the congressman saw the shipyard, which is in the process of being closed and turned over for private development, as a convenient and secure location for his colleagues during the convention. Mr. Weldon, he said, was also eager to promote the shipyard's activities.

So is Richard A. Goldbach, the chairman and chief executive of Metro Machines, one of the largest military contractors at the shipyard. His company is erecting a tent to highlight its work, which includes ship rebuilding and demolition.

"It's pure and simple a promotion," Mr. Goldbach said.

So far, there has been no word from the Democrats, though Pentagon officials they would certainly approve a similar request.

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

AAMVA

KENNETH M. BEAM, CAE
President & CEO

Katherine Burke Moore, Chair of the Board
Deputy Director, Office of Traffic Safety
Minnesota Department of Public Safety

June 1, 2000

The Honorable Steve Horn
Chairman
Subcommittee on Government Management, Information, and Technology
Committee on Government Reform
U.S. House of Representatives
2331 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Horn:

As a follow-up to the Subcommittee's recent hearing on H.R. 220, the Freedom and Privacy Restoration Act, I am enclosing written testimony of the American Association of Motor Vehicle Administrators (AAMVA) on this legislation.

The Association appreciates the opportunity to submit a statement for the record on this matter, and stands ready to work with the Subcommittee as consideration of this measure continues. As you requested, a copy of this statement is also being sent to J. Russell George for inclusion in the record.

Should you have any questions, please feel free to contact me at (703) 908-5766 or via e-mail at llewis@aamva.org.

Sincerely,

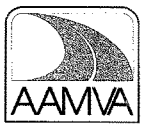
Linda R. Lewis

Linda R. Lewis
Vice President, Government Affairs

Attachment

cc: J. Russell George
Staff Director and Chief Counsel
B-373 Rayburn House Office Building
Washington, D.C. 20515

AMERICAN ASSOCIATION OF
MOTOR VEHICLE ADMINISTRATORS



Written Testimony of the

American Association of Motor Vehicle Administrators

On H.R. 220, the Freedom and Privacy Restoration Act

Submitted to the

Committee on Government Reform

Subcommittee on Government Management,

Information, and Technology

U.S. House of Representatives

Washington, DC

June 1, 2000

4301 Wilson Blvd, Suite 400 • Arlington, VA 22203 • Telephone 703.522.4200 • FAX 703.522.1553

Mr. Chairman, and members of the Subcommittee. Thank you for providing the American Association of Motor Vehicle Administrators (AAMVA) with the opportunity to submit a written statement to the committee on H.R. 220, The Freedom and Privacy Restoration Act.

AAMVA is a voluntary association representing the motor vehicle administrators and chief law enforcement officials in North America. Our members administer the laws that govern motor vehicle operation, the driver credentialing process, and highway safety enforcement. We appreciate the opportunity to brief the Subcommittee on use of the Social Security Number by our members and to discuss how H.R. 220 would fundamentally affect a majority of motor vehicle agencies.

The use of the social security number (SSN) for driver's license issuance or motor vehicle registration was originally authorized in 1976, in Section 405(c)(2)(C)(i) of title 42, United States Code. This authorization was specifically for the purpose of establishing the identification of individuals. In the nearly 25 years since its passage, Congress has consistently used this authority to mandate that state motor vehicle agencies carry out a whole host of federal objectives tied to the SSN. At the same time, some members of Congress have introduced legislation to tighten or rescind this authority. These conflicting congressional objectives have wreaked havoc at the state level, leaving motor vehicle departments caught between battles over using the states to administer federal programs and personal privacy.

As you well know, H.R. 220, which was introduced early in the 106th Congress by Congressman Ron Paul, seeks to repeal the authority of motor vehicle agencies to use the SSN in any way. Passage of H.R. 220 would severely impact the motor vehicle and law enforcement community's ability to ensure public safety by combating document and identity fraud.

Conflicting Federal Mandates

Many federal mandates that DMVs currently work under would be in direct conflict with H.R. 220. Of particular note, Public Law 104-193, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, requires state motor vehicle agencies to collect the SSN for all drivers to help facilitate the collection of child support payments. This requirement takes effect on October 1, 2000 and mandates that states share this data with their state Office of Child Support Enforcement. Congress directed the states to collect this information because it determined that collecting child support from non-custodial parents was a worthy federal objective.

States were also required to collect the SSN under Section 656(b) of Public Law 104-208, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. AAMVA supported Sec. 656(b) because the provision would have gone a long way to enhance the security of the credentials our members issue.

Unfortunately, the public safety and identity protection benefits were ignored as DMVs were accused of creating a national identification card. The reality is that because of the increased fraudulent use of falsified documents, states thought it important to upgrade the minimum security standards of these documents. Sec. 656(b) would have done much to help states enhance the security of their credentials. Contrary to what was portrayed by those opposed to Sec. 656(b), the DMVs were in no way working with the federal government to create a national identification card. Rather, our interest in the provision stemmed from the benefits we saw arising from the new standards in the area of public safety, fraud prevention, and identity theft protection. The Act required the collection of the SSN, but contrary to what was represented in the media, it but did not require states to display the SSN on the license—that decision remained, as it always has, under the purview of individual states.

Nonetheless, support for Section 656(b) disappeared because of privacy concerns surrounding the use of the SSN, but the AAMVA membership has continued the effort to enhance the security of driver license credentials. It is unfortunate that the benefits of Section 656(b) were lost because of the SSN component.

One recent example illustrates just how far the provisions in Sec. 656(b) would have gone to enhance public safety and protect individuals' identity. Just last week, the Senate Governmental Affairs Permanent Investigations Subcommittee, which is chaired by Senator Susan Collins of Maine, held a hearing on the increasing use of the Internet to purchase and manufacture phony driver license and i.d. credentials. The burgeoning availability of false identification credentials on the Internet has a very real public safety impact. When driver license and identification cards are obtained fraudulently, it erodes the states' ability to control the safe operation of motor vehicles on our nation's roadways by allowing unsafe drivers on the road without being tested. Despite the business community's reliance upon driver licenses as a valid form of identification, a driver license is fundamentally intended to represent that the holder is authorized to drive. Fraudulent issuance of driver licenses takes away the ability of the states to control their driving population and protect the safety of their citizens operating on the roadways.

The availability of documents over the Internet means that those who would like to assume another's identity have it all that much easier. We believe that the ease with which false identification documents can be obtained over the Internet is due, in part, to the repeal of Sec. 656(b). Congress acted spuriously in repealing this section as part of the FY 2001 Appropriations for the Department of Transportation. As we have noted previously, Sec. 656(b) would have upgraded states' use of additional security features on driver's license and I.D. cards in order to make them more tamper resistant and make it more difficult for impostors, identity thieves, and scofflaws to obtain fraudulent documents. Many states use a number of both overt and covert security features to detect fraudulent or phony documents, but counterfeiters have kept pace with the technology used by the states. In a sting operation conducted by Senator Collins' staff, false driver licenses, identical to those issued by the state, were obtained from jurisdictions across the country. AAMVA believes that the regulations to implement Sec. 656(b) would have

gone a long way to enhance the security of state-issued driving credentials by encouraging states to use as many security features as possible on their documents. This, in turn, makes it more difficult for the bad seeds to continue their fraudulent activity.

Why Do States Need to Use the SSN?

When obtained in conjunction with the name, date of birth and gender, the SSN enables DMVs to positively identify a person on the agency's driving record files. This helps to minimize the possibility that erroneous information, such as accidents or convictions, will be placed on the wrong person's driving record.

Today, motor vehicle agencies maintain the driver history records of more than 200 million vehicle operators in the United States alone. AAMVA believes that the use of the SSN as a unique identifier is necessary to maintain accurate records and to prevent harm to individuals and businesses as a result of misuse of official credentials. It is important for us to note that these credentials include not only documents such as the driver's license that are widely used and accepted for personal identification, but also documents that evidence ownership and other property interests in motor vehicles, such as registrations and titles.

The SSN also is used as a common identifier to facilitate electronic data exchange among motor vehicle agencies and other authorized users. Omitting the social security number as an identifier could result in inaccuracies in driver information retained and exchanged among states and could seriously jeopardize highway safety. Without an effective way to ensure data is correctly applied to the right driver record, useful data exchange will be compromised. The tendency today, particularly with driver record information, is to institute an even greater exchange of driver history data among the states as a means to enhance the safe operation of motor vehicles and ensure that bad drivers do not continue to operate their vehicles.

One case in point is the recently passed Motor Carrier Safety Improvement Act of 1999 (Public Law 106-159). This legislation mandates that the courts begin sharing commercial operator conviction data with state motor vehicle agencies—regardless of whether the violation occurred in a commercial motor vehicle or a passenger vehicle. As the borders between the U.S., Canada, and Mexico open under the North American Free Trade Agreement, the association believes that state DMVs will be called upon to share driver records with those countries to ensure that only licensed qualified drivers operate across the border.

The Commercial Motor Vehicle Safety Act of 1986 (CMVSA) mandated the creation of the Commercial Drivers License Information System (CDLIS). CDLIS provides the electronic means to share commercial driver histories among the states and other authorized users. The CMVSA also mandates that the SSN be used as the unique identifier for commercial drivers' records on the system. All 51 U.S. jurisdictions operate CDLIS. All collect the SSN for commercial drivers as the federal law requires. Prior to the establishment of CDLIS, commercial drivers could obtain CDLs from multiple

jurisdictions. Once a CDL is withdrawn in one state, the driver loses his or her privilege to operate a commercial vehicle in every other state. Prior to CDLIS, states had no way to check whether the individual held any other commercial license and in some cases individuals who had lost their CDL privileges in one state simply continued to drive with a valid license from another state. The operation of the CDLIS system has virtually eliminated the problem of multiple CDL licenses.

AAMVA has long supported the "one driver—one license" concept for all drivers. We encourage Congress to support the establishment of the Driver Record Information Verification System (DRIVerS) that will enable motor vehicle agencies to ensure that ***all*** drivers do not have more than one driver license and to accurately post conviction data to the record associated with that license. Until we are able to query such a system prior to the initial issuance of a driving credential or upon renewal, the deceptive practice of obtaining multiple passenger licenses to unlawfully distribute traffic citations and violations among them will continue.

Congress provided funding under TEA-21 to undertake an assessment of available electronic technologies to improve access to and exchange of motor vehicle driving records. One element of the assessment will be to review alternative unique motor vehicle driver identifiers that would facilitate accurate matching of drivers and their more than 200 million records. Some unique identifier is necessary for the states to carry out their safety mission. The SSN has proved itself to be an effective tool in uniquely identifying drivers that pose a safety risk. Repealing the authority of DMVs to use the SSN for secondary identity verification would severely jeopardize the ability of such a system to fulfill its purpose.

From the motor vehicle agencies perspective, the problem is very clear in the driver license administration arena: without a standardized unique identifier, the ability to electronically transfer driver record information and take action against those drivers who jeopardize highway safety will fail.

SSNs are for Identity Verification, Not Tracking

AAMVA, through its subsidiary organization AAMVAnet, provides an electronic data exchange application through the Social Security Online Verification system (SSOLV) to assist states in the identification verification process for a driver license credential. This system allows DMVs to send an individual's name, date of birth, and SSN to the Social Security Administration (SSA). The SSA, in turn, verifies that information against its Master File and reports back to the requesting DMV whether or not the DMV information did or did not match the information on file at the SSA. Currently, eight jurisdictions are in production at this time through a Memorandum of Understanding with the SSA.

This on-line support allows a jurisdiction to instantaneously verify an individual's SSN during the driver license issuance or renewal process while the driver is still at the

counter. AAMVA believes that this will help cut down on fraud and make it more difficult for an imposter to obtain fraudulent documents.

Individuals Have the Option to Not Display their SSN

In recent years, the public's concern about the privacy of personal information stored in their driver's license records has caused many motor vehicle agencies to change their policies about displaying the SSN on the driver's license. Today, 49 states either do not display the SSN or give the public the option of using a state issued alpha-numeric identifier. However, the SSN remains an important identifier for electronic driver record exchange and recordholder verification. Jurisdictions may not disclose the SSN to third parties without the express consent of the individual (with limited exceptions for law enforcement and the courts, etc.), and the SSN is primarily used behind-the-scenes as a tie-breaker when an individual with a very common name comes to a DMV. Without the ability to link a person to a unique identifier such as the SSN, DMVs would be confronted with literally thousands of matches for "John Smith" or other common names. We believe this problem will become particularly problematic in the Latino community where there is a large commonality of names.

In closing, we would like to reiterate the importance of using the SSN for issuance of driver license credentials and other property documents. The public safety benefits of SSN use are numerous and far outweigh any potential disadvantages.

We urge the Congress to consider these invaluable uses and not restrict the motor vehicle and law enforcement community from utilizing the SSN as the unique identifier for the millions of driver records we administer.

We appreciate the opportunity to submit written testimony and will be happy to respond to any additional questions the Subcommittee may have. Please call AAMVA's Vice President of Government Affairs Linda Lewis at (703) 908-5766 or by e-mail at llewis@aamva.org.

○