

Y 4
.J 89/2
96-75

1042

96 Y 4
J 89/2
96-75

COMPUTER SYSTEMS PROTECTION ACT OF 1979, S. 240

GOVERNMENT
Storage



HEARING
BEFORE THE
COMMITTEE ON CRIMINAL JUSTICE
OF THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
NINETY-SIXTH CONGRESS
SECOND SESSION
ON
S. 240

FEBRUARY 28, 1980

Serial No. 96-75

Printed for the use of the Committee on the Judiciary

DOCUMENTS



MAR 11 1981

FARRELL LIBRARY
KANSAS STATE UNIVERSITY

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1980

69-082 O

AY
2/28/52
27-28

COMMITTEE ON THE JUDICIARY

EDWARD M. KENNEDY, Massachusetts, *Chairman*

BIRCH BAYH, Indiana
ROBERT C. BYRD, West Virginia
JOSEPH R. BIDEN, Jr., Delaware
JOHN C. CULVER, Iowa
HOWARD M. METZENBAUM, Ohio
DENNIS DeCONCINI, Arizona
PATRICK J. LEAHY, Vermont
MAX BAUCUS, Montana
HOWELL HEFLIN, Alabama

STROM THURMOND, South Carolina
CHARLES McC. MATHIAS, Jr., Maryland
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ROBERT DOLE, Kansas
THAD COCHRAN, Mississippi
ALAN K. SIMPSON, Wyoming

STEPHEN BREYER, *Chief Counsel*

EMORY SNEEDEN, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIMINAL JUSTICE

JOSEPH R. BIDEN, Jr., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOHN C. CULVER, Iowa
DENNIS DeCONCINI, Arizona
PATRICK J. LEAHY, Vermont

CHARLES McC. MATHIAS, Jr., Maryland
THAD COCHRAN, Mississippi
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah

MICHAEL GELACAK, *Staff Director*

MICHAEL GITENSTEIN, *Chief Counsel*

KATHY ZEBROWSKI, *Counsel*

DOCUMENTS
MAR 1 1952
FARFALL LIBRARY
IOWA STATE UNIVERSITY

CONTENTS

THURSDAY, FEBRUARY 28, 1980

STATEMENTS

	Page
Opening statement of Senator Hatch.....	1
Opening statement of Senator Laxalt.....	2

TESTIMONY

MacFarlane, Hon. J. D., attorney general, State of Colorado.....	5
Dertouzos, Prof. Michael, Massachusetts Institute of Technology Laboratory for Computer Science.....	17
Taber, John K., programmer, Santa Clara, Calif.....	39
Falke, Lee, chairman of the board, National District Attorney Association.....	52

PREPARED STATEMENTS

Dertouzos, Prof. Michael.....	26
Taber, John K.....	47

APPENDIX

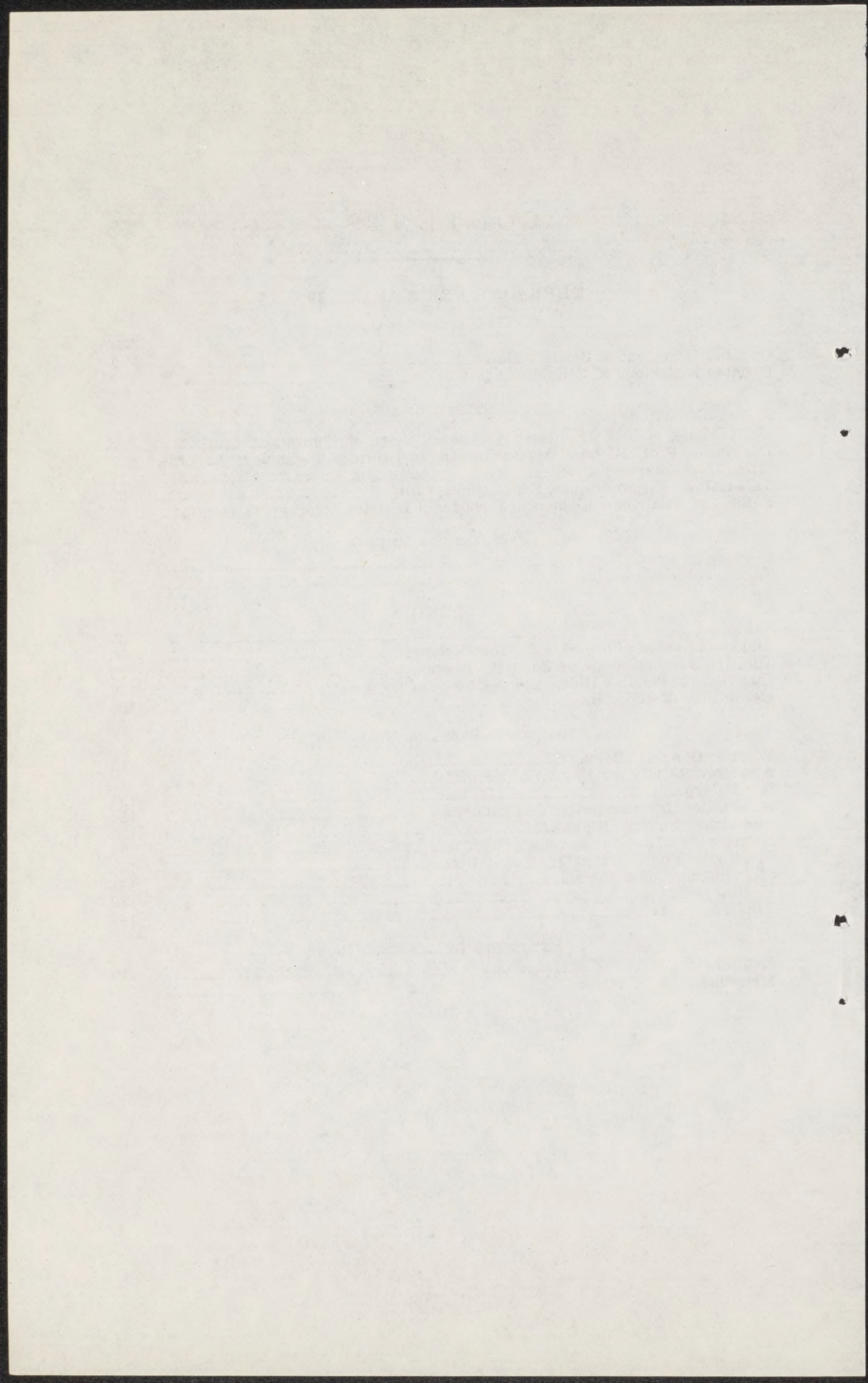
S. 240.....	59
Additional submissions of J. D. MacFarlane.....	65
Additional submissions of John K. Taber.....	72
Questions of Senator Biden and responses of the FBI.....	106
Resolution of the ABA.....	108

ADDITIONAL PREPARED STATEMENTS

Wayne Douglas Bennett.....	115
American Society for Industrial Security.....	117
Rand Corp.....	131
Association for Computing Machinery.....	134
Greenwich Savings Bank.....	135
Nationwide Financial Services Corp.....	136
Electronic Funds Transfer Association.....	138
SRI International.....	141
H. Stuart Knight.....	143
CBEMA.....	147

EXHIBITS AND MISCELLANEOUS

Exhibits.....	149
Miscellaneous.....	155



COMPUTER SYSTEMS PROTECTION ACT OF 1979, S. 240

THURSDAY, FEBRUARY 28, 1980

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The committee met, pursuant to notice, at 10:35 a.m., in room 6226, Dirksen Senate Office Building.

Present: Kathy Zebrowski, counsel to Senator Biden; Stephen Markman and Renn M. Patch, counsels to Senator Hatch; and Jock F. Nash, Jr., counsel to Senator Laxalt.

Mr. MARKMAN. Could we please call the hearing to order.

My name is Steve Markman. I am minority counsel for the Judiciary Committee.

As we have explained to the witnesses, a number of unexpected events this morning have made the presence of the Senators impossible. A last minute hearing has been scheduled on a very important matter that is taking place elsewhere in the Judiciary Committee.

In addition seven rollcall votes are presently being taken on the floor that should consume the next hour and a half. The Senators on the committee expect to be here as soon as they possibly can, but in the best interests of this hearing, we will presently get started.

I would like to read the opening statement of Senator Orrin G. Hatch, of Utah.

OPENING STATEMENT OF SENATOR HATCH

Senator HATCH. The subject of today's hearing is Senate bill 240, The Federal Computer Systems Protection Act. I would like to extend my sincere appreciation to the distinguished chairman of the Senate Judiciary Committee, Senator Kennedy, and its Criminal Law Subcommittee chairman, Senator Biden, for allowing my distinguished colleague from Nevada, Mr. Laxalt, and myself to hold this day of hearings. It is the first such day of hearings that have been held on S. 240 during the present Congress.

There are two major concerns that I presently have about this legislation. Among the purposes of today's hearings are to pursue these concerns with the able and respected panel of witnesses that have consented to testify here.

First, I believe that the threshold question must be addressed as to the need for this legislation. According to the U.S. Department of Justice, there are 40 sections of the United States Code, provisions of the Electronic Funds Transfer Act, provisions of the Financial Institutions Act, and provisions of the Privacy Act, that have direct

utility to Federal prosecutions of computer abuse. What then is the compelling need for this legislation?

At the same time that Senate bill 240 is being considered by this committee, our committee is also preparing for consideration on the floor of the Senate of a comprehensive criminal code reform measure. This reform is prompted by the amount of statutory overlap and inconsistency and duplication that has grown in the criminal laws of the country for many years.

I feel compelled then to ask whether or not S. 240 represents a first step down the same path again. What are the gaps in the present law? What difficulties do Federal prosecutors have in working with the present law? Will Senate bill 240 enable us to consolidate or repeal provisions from these earlier laws? Each of these questions, among others, must be clearly answered, in my opinion, before we can justify enacting yet another statute.

Further, the burden is on those who desire this new legislation.

Second: I am concerned about what might be a significant expansion of Federal jurisdiction represented by Senate bill 240.

I am particularly concerned in view of the fact that computer technology is likely to become increasingly pervasive in the near and distant future. Will Federal criminal jurisdiction grow as computer use grows? Will Federal responsibility develop in areas presently within State and local jurisdiction simply because a computer rather than an automobile or shotgun is the subject of a crime? These questions must be addressed in greater detail than they have been thus far.

I am not insensitive to the growing use of sophisticated computers in perpetrating criminal activity. Nor am I insensitive that far greater expertise is needed among law enforcement officers at all levels if we are going to be able adequately to deal with this criminal activity. I am not necessarily or unalterably opposed to Senate bill 240. I simply believe that this is too important a piece of legislation to expedite without full committee consideration.

I would also like to extend my appreciation to the chairman of the subcommittee, Mr. Biden, for his cooperation with Senator Laxalt and myself in accepting several of our amendments that we offered at the subcommittee level. These included revisions aimed at limiting the Federal liability of those whose only nexus with the Federal Government is that of sharing time on a computer used by the Federal Government; excluding certain types of computers from the purview of the act, including automatic typewriters or typesetters, and computers designed for routine personal, family, or household use; and requiring the Federal Government to consider various factors prior to exercising Federal jurisdiction where that jurisdiction is held concurrently with the States.

I extend my gratitude to the witnesses for taking time out of their busy schedules to be with us today. I am sure we will all be able to benefit by their expertise.

I think that John Nash, minority counsel with Senator Laxalt would like to read Senator Laxalt's opening statement at this point.

OPENING STATEMENT OF SENATOR LAXALT

Senator NASH. Today, the Senate Committee on the Judiciary opens hearings on S. 240, the Federal Computer Systems Protection Act of 1979.

The legislative history of S. 240 goes back to June 22, 1977, when it was first introduced in the 95th Congress as S. 1766. Two days of hearings were held on June 21 and 22, in 1978, but the bill failed to be reported out of the Senate Committee on the Judiciary before the end of the second session.

The bill was reintroduced in the 96th Congress as S. 240, on January 25, 1979. It was then referred to the Criminal Justice Subcommittee where it underwent extensive amending. The subcommittee members agreed to report the bill to the full committee toward the end of 1979, with the provision that further hearings would be held at that level.

In December of last year, the Senate Committee on the Judiciary reported favorably to the full Senate S. 1722, the Criminal Code Reform Act of 1979. This was a massive and ambitious undertaking whereby the Judiciary Committee reformed and codified the entire body of the Federal substantive and procedural law contained in title 18 of the United States Code. This process took more than a decade to accomplish, and the bill is now awaiting floor action in the Senate.

During the hearings and debate on that bill, there was nothing that caused more heated debate and serious inquiry than when a new substantive offense was added to the Criminal Code, excepting perhaps, the issue regarding the ever-expanding scope of Federal jurisdiction.

S. 240, the Computer Systems Protection Act of 1979 contains the elements of both of those controversies. The bill not only adds new substantive offenses to the Criminal Code, it expands Federal criminal jurisdiction in such a way that the "wire and mail" fraud statutes pale by comparison.

At the present time, along with the Electronic Funds Transfer Act, title XX of FIRA, and the Privacy Act of 1974, there are 40 sections of title 18 of the United States Code that are being utilized by Federal prosecutors to bring the computer felon to justice.

With these considerations in mind, I have joined with Senator Hatch to conduct this hearing to further investigate the utility and the necessity of adding yet another substantive criminal offense to the Federal Criminal Code.

There are, I believe, at least four areas of concern regarding the Computer Systems Protection Act. The first I have mentioned, and that is to what extent will S. 240 expand Federal jurisdiction into areas traditionally reserved to the States?

Second: What is the evil to be remedied? What is the incidence of computer crime and what are its costs to our society?

Third: By focusing on the computer as an instrumentality, are we exposing individuals to criminal liability for possibly innocent conduct while not furthering the public safety and welfare?

Finally: Does S. 240 properly define the context in which a computer may be viewed as a possible instrumentality of criminal acts? Has Congress properly understood the intricacies and dimensions of a very complex question?

The Federal Government has the power to create statutory crimes as to conduct within the United States because the Constitution gives Congress the power to do what is "necessary and proper" to carry out the various expressly conferred powers, such as the power to regulate interstate commerce, to tax and so forth.

The scope of Federal substantive criminal law of this variety has been growing steadily since this Nation was founded. Some feel the expansion of Federal jurisdiction has grown out of the proportion to its need.

In the past, the Federal Government has exercised its jurisdiction to punish antisocial conduct of primarily local concern, conduct with which the local police are often unable or unwilling to cope. Thus transporting a stolen automobile—or a woman for immoral purposes or a kidnaped person—across a State line is made a Federal crime, although it is in actuality, the car theft, a local matter, rather than the incidental act of transportation across a State border, which constitutes the real evil to be combated. The kind of public outrage that precipitated the expansion of Federal jurisdiction embodied in the Mann Act and the Lindbergh kidnaping law is not as apparent with regard to this computer crime bill.

S. 240 as now drafted seems to enable the Federal Government to intervene in virtually every instance of criminal conduct associated with the computer. The threshold question that must be addressed is whether or not the States are ready, willing, and able to bring their prosecutorial resources to bear on computer related crime that comes to their attention in their respective jurisdictions.

This committee is fortunate to have as witnesses, both the president of the National Association of Attorneys General and the chairman of the board of the National District Attorneys Association with us today. I am confident that these two gentlemen will be able to shed some light on this aspect of the problem.

A second important area that warrants serious committee inquiry is determining the actual incidence of computer related crime. I have seen widely disparate estimates of its cost to society.

For example, Prof. August Bequai—who assisted in the drafting of this bill—wrote in his book "Computer Crime" that the computer felon "steals more than \$100 million annually from our citizenry."

Professor Bequai further states that "fewer than 1 percent of all computer crimes are uncovered. When finally discovered, the felon escapes justice by simply taking advantage of the legal maze we have created."

However, the recently published Criminal Justice Resource Manual on Computer Crime prepared for the Department of Justice, states on page 129, that prosecutors have found statutes "to prosecute all cases of computer related crime coming to their attention." Perhaps during our hearing today we will discover where the truth lies. It is of paramount importance that this committee know where the gaps in present law are so that we can fill them in a timely fashion.

There is a mystique regarding the computer that has allowed a rather extensive lore of mythology to accumulate around it. There is no functional difference between a file cabinet and a computer. Both store information albeit to a different degree.

Accepting this analogy for purposes of discussion, why should someone be treated differently for stealing information out of a file cabinet than a person who takes the same information from a computer?

Is one theft less socially desirable than the other?

Are there such significant differences that one larceny must be treated differently than the other for purposes of prosecution?

Should the computer theft be given a special status such that the legal penalties for the perpetrators are correspondingly different? It seems unwise to create such anomalies of law.

Finally: We come to the issue of whether this legislation takes into account the intricacies of this highly specialized and considerably complex field of technology. I believe there is a need for some sort of Federal criminal statutes in this area. My concern is how that statute should be drafted. We found at the subcommittee level that even the computer industry differs on how you define the term "computer." If this is indeed the case, I look forward to this morning's testimony in hopes that we can make a record which will assist this committee in its work.

Mr. MARKMAN. Our first witness will be the Honorable J. D. MacFarlane, attorney general of Colorado.

Mr. Attorney General, before you begin, can I just state again that we are sorry that the Senators are not here.

I do want to clarify for the witnesses today that the testimony taken here will be submitted to the members of the subcommittee. It will be submitted to the members of the full committee and considered thoroughly by members of the committee and by their staff.

I would like to emphasize that today's hearing is particularly important because it is likely to be the only hearing that will be taking place this year on Senate bill 240.

I would also like to introduce up here, Ms. Kathy Zebrowski, who is majority counsel for the chairman of the subcommittee, Senator Biden.

Mr. Attorney General, would you like to begin?

**STATEMENT OF HON. J. D. MacFARLANE, ATTORNEY GENERAL,
STATE OF COLORADO**

Mr. MacFARLANE. Thank you, Mr. Markman.

Let the record show I am J. D. MacFarlane, attorney general of Colorado and president of the National Association of Attorneys General.

The statement I will make this morning does not necessarily reflect the position of the National Association of Attorneys General inasmuch as our executive committee has not yet taken a formal position on this bill.

I further state for the record, I am sorry that I do not have a prepared statement to submit. Unfortunately, by the time I was notified and asked to testify on this bill, with intervening matters taking place, I was unable to get my thoughts down into writing. However, that may be remedied by the record.

I think it is a proper thing to start out this inquiry with the question that both Mr. Markman and Mr. Nash have raised in their respective statements of their respective Senators, and that is: Why do we need this law?

I think the quickie answer is, and I will expand on this, that because there ought to be a law.

In short, the thrust of my testimony is going to be I don't see that there has been sufficient proof of the need for a specific statute on

computer crime to justify the tremendous implications that are contained in the language of this existing bill.

As has been mentioned already in the testimony that the Justice Department of the United States has submitted in hearings on S. 1766, on June 21 and 22, 1978, there are some 40 statutes now in existence in the Federal jurisdiction that cover one or another aspect of computer crime.

I might also note that in the 12 States to my knowledge that have enacted computer crime bills similar or analogous to the proposed Senate bill 240, there have been no indictments and no convictions obtained under any one of those bills. I don't know all of the information on it, and certainly my State is one that has such a bill, or such a law.

So we are in a very experimental situation. We don't know what is going to turn up in those jurisdictions that have enacted computer fraud bills. We don't know what problems of proof, what problems of investigation, how the courts are going to rule in areas where there is no question of or no issue of how broad should the jurisdiction be.

In short, we don't know. I submit that none of us really know what the implications of this legislation are. I am going to suggest a few this morning.

I have an article that I examined on computer crime by John Taber, IBM systems programmer. It appears in the *Computer Law Journal*. I am sorry I do not have the date of it. I can provide copies. It is 1979, volume 1. I think this should open this speculation.

He says in the concluding paragraph to that article:

The fundamental flaw of the proposed Federal legislation is that the bill defines an abstraction. Computer crime is a crime. Rather than proscribing specific acts the phrase "computer crime" or "filing cabinet crime" beclouds specific criminal acts and noncriminal acts with that drawn from the instrumentality of the act.

Now this is extremely important to understand. While it is true that one may commit murder with a filing cabinet by dropping it on the victim, and one may tamper with records by using a computer; nevertheless, the crimes are murder and fraud, not unauthorized use of a filing cabinet or unauthorized access to a computer.

What are we dealing with in the area of computers today? What are we really trying to get after when we say that computer crime, if it is not already, ought to be a crime?

Let me suggest the following language may clarify this question somewhat. It appears in a publication called *Computer Crime*, a criminal justice resource manual, published by the Law Enforcement Assistance Administration, U.S. Department of Justice, at page 9. They are talking about computer related crime methods and detection. The following language I think is important to understand.

Like most aspects of computer technology, a jargon describing the now classical methods of computer-related crime has developed. These are the technical methods for some of the more sophisticated and automated computer related crimes.

The results are modification, disclosure or taking, destruction and use or denial of use of services, computer equipment, computer programs or data in computer systems.

Depending upon the meaning of the data, kinds of services or purpose of the program, the acts range over many known types of crime.

We are talking about modification, disclosure, alteration, access of records. What we are really dealing with in terms of computer technology are gigantic filing cabinets and ways of manipulating the documents in those filing cabinets and the information that is contained therein.

Now, I submit that that is no different than a very large warehouse full of filing cabinets with documents in it, with people that can access those documents and alter them or take them or take pictures of them and use them for some illegal purpose that is already defined and made criminal by either State or Federal statutes. Once we understand the nature of what computers are, which is simply gigantic information banks, then we can better understand what we are talking about when we talk about computer crime.

Now what are some of the implications of making computer crime a specific Federal crime? By way of illustration let me suggest what the state of the art is now in terms of the law business.

Most large law firms and eventually all law firms and all lawyers are and will be doing most if not all of their legal research via computer. The Lexis system, the Westlaw system, the Juris system are but beginning and elemental examples of that.

The technology is here, in effect, to browse through the Library of Congress by a word search, never opening a book and never looking at an index catalog and to retrieve the universe of the documents in the Library of Congress, in moments, relating to a specific subject matter of search. All it takes is a slight bit of training to be able to do this.

Thus, I am saying that in the near future lawyers will do all their legal research by a cathode ray terminal and a simple printout device. They will not use books.

The average law firm today, if it is not already doing so, will keep all of its time documents, timekeeping by which they bill clients via computer. Even Government agencies are doing this, mine is one. Bookkeeping, keeping the ledger accounts is done via computer.

Word processing—in my office in Colorado we produce very few documents any more—briefs, memoranda, what have you—by any means other than a computer. By this I mean a main frame computer, by which we can manipulate text and do all sorts of interesting things. That is what will happen with every law firm and lawyer in the country. We won't have typewriters any more.

The day is not far off when we will be dictating into a telephonic device and, via a computer program, that will be transcribed into computer readable language and will be printed without the intervention of the human hand.

We are proceeding and are very near to achieving the so-called paperless office. Internal memoranda, such small things as telephone notes, will simply be entered into a computer either by dictation or via cathode ray terminal and will be transferred back and forth from lawyer to lawyer, staff member to staff member via the terminals. Electronic notes to yourself about things to do will be done the same way.

Even if a stray document in the future comes in hard copy, it will immediately be read by an OCR device and logged into the computer,

instead of a mail logging process which is common today, and will be transferred to the proper attorney or the proper staff member via that person's own individual CRT.

In short, every single item of communication in a law office that now exists, short of direct oral communication from one person to another, will be done electronically. It will be stored electronically. It will be accessible electronically. Now that is just in the law business. What I am saying about the law business is that everything will be done via computer, short of oral argument in court.

Now extend this to every other business in this country or every other Governmental occupation or endeavor that uses paper as a means of communication. We will not be using the mail. We will be transmitting instruments electronically over telephone lines or via satellite. We may not even see hard documents at any point because all these matters will be accessible via a cathode ray terminal and displayable on a screen. In a way it is the reverse of the paper flood that the Xerox 914 created in the early 1960's.

But what will be there are gigantic computer files. The technology exists today to store information along the order 10^{15} bits on a matrix device, 1 meter square, accessible at electronic speeds, which means that the one major block to storing everything like the Library of Congress documents on a computer is just around the corner.

The only thing that Senate bill 240 exempts from this process in terms of potential jurisdiction are computers for home use purposes, and even that exemption isn't complete. Because in the technology of today, though it may not be used, people are going to have computers in their home that are going to be tied in with their bank accounts when they want to dial the proper number, or their supermarket, and any one of a number of other uses your imagination can devise. So they won't be purely limited to home use at all.

It doesn't seem to me that the definition that is now contained in the bill which allows—which defines the uses of the computer that can be reached as operating in or using a facility of interstate commerce—really excludes very much.

Robert Bigelow, in an article in the January 1980 Computer Law and Tax Report, comments on this aspect of the bill. His comment is on page 4, of the January article, that the phrase "operates in or uses a facility of interstate commerce means that every network and remote system is covered as is every off-line system that receives or programs data by mail or truck."

Now I submit that doesn't exclude very much.

There is very little, in sum, it seems to me, of the various aspects of computer crime, what one would like to catalog as computer crime, that is not already covered by an existing criminal statute if one examines what is the purpose of the criminal act and doesn't get all hung up simply because things are done electronically as opposed to other time tested methods.

Therefore, I am going to suggest that if there is a need for this bill that the bill be amended to include only computer operations, uses, et cetera, exclusively used for purposes of the Federal Government.

I am going to suggest some amendments to achieve that objective. Because if indeed there is a problem here, I think we ought to find out the extent and ramifications of such a bill in a relatively discrete and

limited area which no one will contest is the business of the Federal Government; and find out through operating and through some history, just exactly what this kind of thing is going to cover and what the implications of it are going to be.

The amendments I would suggest, therefore, of Senate bill 240, begin in paragraph 1, of the substantive offense definition where the bill defines the scheme or artifice to defraud and so on, if the computer, subparagraph 1, is owned by—I will read the language as I would have it finally appear and then suggest what would be stricken or added to get there.

I would suggest the language should read in paragraph 1:

Is owned by or operated directly for or on behalf and for the exclusive use and benefit of the U.S. Government; and the prohibited conduct directly involved or affects the computer operation directly for or on behalf of the U.S. Government.

Strike subparagraph 2. I think that that would sufficiently limit the jurisdiction to Federal Government itself, computers operated directly by or on behalf of it, for its exclusive use and benefit.

I would suggest that Mr. Taber, in the article I have already referred to, page 519, points out that there are some reported instances of such exclusive Federal "computer crime."

On page 519, he says:

From information supplied by many Federal Government investigative agencies, the Government Accounting Office has reported the total of 69 cases of computer crime in the entire Federal Government.

Actually, there were only 66 reported cases since the Air Force erroneously identified three cases as computer crimes that did not even involve computers.

Nine of these 66 cases involved no dollar loss, being incidents such as privacy invasion. The total reported losses were \$2,161,412. The average loss was \$44,000. The median loss was \$67,149.

I would suggest that that is enough computer crime, in view of the sophisticated nature of computer crime, for the Federal Government to develop a data base on which to judge whether this act ought to be extended any further than the Federal Government.

I could, but will not, suggest that there ought to be a gradation in terms of the substantial nature of the offense which there is not now. The reason I don't suggest that is I think that if the impact of my suggested amendment to this bill is first tested in Federal Government agencies, then it is entirely possible those in charge of prosecuting those crimes or those in charge of passing the laws resulting in such crimes will come to the inevitable conclusion there are petty crimes and there are major crimes and there ought to be some gradation. But since the present proposed legislation doesn't make that gradation with regard to anyone, if my proposed amendment were to be adopted, I think the Federal Government would be a good test case to test out the substantial nature of those penalties.

In conclusion, I would like to note that my remarks can be summed up by remarks made by the chairman of this Judiciary Committee in a recent talk to the Massachusetts Bar Association wherein he said:

Crime is primarily a State and local problem that will not be resolved in Washington. The most appropriate Federal rule is to try to put our own house in order while encouraging the 50 States to experiment and to seek to innovate responses to the problem of crime in America.

Obviously, what I have suggested by my amendment is that we do just that and let your experiment be on the Federal Establishment and

not on the rest of us poor jokers out in the countryside that don't even realize that there is such a thing as computer crime. We do realize that it is wrong to steal and that it is wrong to cheat and that it is wrong to mislead. That is not hard to understand. I think we can handle that under either our current laws or a State law on computer crime.

Thank you.

Mr. MARKMAN. Thank you Mr. MacFarlane. You have raised some very provocative questions. I know it is going to be very useful to the members of the committee.

I will ask you just a couple very quick questions. The standard rebuttal to the attempt to analogize the filing cabinet and the computer as vehicles for committing criminal offenses tends to be that crimes involving the computer as opposed to crimes involving the filing cabinet tend to be of a much more highly sophisticated variety, and that the detection and prosecution of those crimes also tends to be of a more highly sophisticated variety.

In your view, do you believe the States presently have the resources, or the abilities to develop the resources, to deal effectively with what we understand to be increasingly sophisticated instances of computer crime?

Mr. MACFARLANE. I certainly do. I don't view the problems of computer crime or, more accurately, crimes involving the use or operation of computers to be any more sophisticated or any less, for that matter, than the problems of detecting and prosecuting an antitrust violation or an organized crime conspiracy. They are all difficult.

The basic problem which relates all those three together, crimes involving computers, antitrust violations, and organized crime, is that they are crimes difficult to detect because they are perpetrated by intelligent people. Often enough the real problem isn't in the prosecution or investigation, the problem is simply knowing whether in fact a crime has been committed. The problems of detecting it, getting information on it, are similar.

We in Colorado have had occasion in antitrust price-fixing cases to get our best information from disgruntled former employees, inside informants. The one computer-related fraud that we were involved with came from a similar source. The company didn't know it, what was going on. Nobody knew it but a couple of people involved in the use of the computer. Some guy got cheated because he didn't get his cut and turned them in.

The same thing is true in organized crime. What I am saying is that you almost always develop those cases from somebody who talks—he knows what the scheme is or the scam. And at that point, if you need an expert, such as a systems analyst, programmer, hardware man, you go get an expert who does it every day and let him guide you and tell you what it is and how it is being done.

I don't see any degree of higher difficulty in detecting and prosecuting so-called computer crime than I do antitrust violations and organized crime and we do that all the time anyway.

Mr. MARKMAN. You would, I take it, on the basis of your statement, see a sharp increase in the amount of jurisdiction held concurrently by the Federal and State governments upon passage of legislation such as S. 240?

Mr. MACFARLANE. Not the State governments, the Federal Government.

Mr. MARKMAN. Pardon me.

Mr. MACFARLANE. I would see a sharp increase in the jurisdiction of the Federal Government.

Mr. MARKMAN. Right.

Mr. MACFARLANE. Yes, because as I tried to point out, practically everything if not today, tomorrow, in terms of communications, is going to involve computers. That gives Federal jurisdiction over all communications conducted via computer. If all communications other than oral are going to be conducted by a computer as I postulated, that is virtually 99 percent of our communications that you are going to have jurisdiction over for a Federal crime.

Mr. MARKMAN. So if we were going to maintain something roughly akin to the present balance of jurisdiction between the Federal and State governments, it would at that point rest increasingly upon prosecutorial discretion by the Federal authorities and nothing more than that?

Mr. MACFARLANE. That's correct.

One of the difficulties with that, I might add, is not necessarily involved with the actual filing or indictment of a criminal case, but the initial allegation by some person that may or may not be responsible that such and such is taking place and thus subjecting that activity to scrutiny by investigation. In fact, nothing may be taking place, but in the process of the investigation, just as in the execution of a search warrant, you may run across all kinds of information which a given business person might not want divulged for good and sufficient reasons.

Nevertheless, you have an investigator riffling through all the file cabinets, all personal documents, all financial information. I just see this as, in a way, 1984 come 4 years early.

Mr. MARKMAN. I would like to ask just one more question that Senator Hatch is very interested in. I believe there is something in the order of eight or nine States that have adopted their own variety of computer crime legislation. Are you familiar with the experiences of any of these States and if you are, what difficulties have arisen in the enforcement of these laws? Can these difficulties be corrected short of Federal legislation?

Mr. MACFARLANE. I am only directly familiar with Colorado. I am aware that a dozen States have passed such laws. As I said earlier, I am unaware of any single indictment or conviction under any one of these laws. Specifically, in Colorado, I know that there have been no indictments, much less convictions, under our Colorado statute. It is only 1 year old. There has been no experience. We don't know how the courts are going to construe it. We don't know what it is going to cover.

One difference in our Colorado statute, of course, from S. 240, I referred to earlier, that at least it provides a gradation, depending upon the severity of the offense.

Let me just, for your information, give you that.

If the loss—I am quoting from the Colorado revised statutes, 1973, 18-5.5-102, subparagraph 3.

If the loss, damage or thing of value taken in violation of this section is less than \$50, computer crime is a class 3 misdemeanor.

That is the lowest class of misdemeanor.

If \$50 or more, but less than \$200, computer crime is a class 2 misdemeanor.

If \$200 or more, but less than \$10,000, computer crime is a class 4 felony.

A class 4 felony in Colorado is next to the bottom in our list of felonies.

If \$10,000 or more computer crime is a class 3, felony.

I suggest that that scheme of things, even if our statute ultimately is over broad—and we do have an unauthorized use section in our statute—that at least there is some sense that the punishment ought to fit the severity of the crime and that it would be certainly within prosecutorial discretion using standard plea bargaining, using standard charging techniques, to decide whether or not a particular act in question was serious, not so serious, petty, et cetera.

So that even if the statute does reach more things than maybe it should, at least there are some ameliorating factors in the penalty section.

Mr. MARKMAN. Thank you very much.

Senator Laxalt's office.

Mr. NASH. Thank you.

Attorney General MacFarlane, how long has the Colorado statute been on the books?

Mr. MACFARLANE. It was passed the last session, last year.

Mr. NASH. Are you familiar with the legislative history? It didn't come about in a vacuum?

Mr. MACFARLANE. No.

Mr. NASH. Did you have occasion to testify on that bill when it was being drafted?

Mr. MACFARLANE. I did not testify on the bill. I did not propose the bill. The bill was proposed by the District Attorney's Council. I am not really—I do not really know what the genesis of it was. I do know that we had a supreme court decision in Colorado that involved the question of whether or not the theft laws included the taking of a picture of a confidential file, not removing the document itself from the files. A criminal charge was brought and ultimately dismissed by the supreme court, thrown out, on a ground that there wasn't any taking. The legislature had not defined the mere looking at or copying of a document—so long as there wasn't an actual physical removal of it—as being anything of value.

Now, to my knowledge, that decision is unique in the country and, to the extent that decision sparked our computer crime bill, it is possible that there was some impact there.

I would suggest that if that had anything to do with it, that was not a case even involving a computer, but it was certainly analogous enough so that in the situation where one were to commit a computer crime by for instance accessing a data bank and simply copying that information, transferring it, but leaving the data otherwise intact in the computer file, that the Colorado law, under our supreme court case that I mentioned earlier, would say that there is no crime. To that extent, our computer crime bill covered that loophole.

Mr. NASH. Has Colorado developed a program whereby your law enforcement personnel go through any special training or education to detect computer crime as a result of your legislature's enactment of the last session?

Mr. MACFARLANE. I really—I don't know what the status of the district attorneys or—I know what the status of our organized crime strike force and our Colorado bureau investigation is. The answer is no. I qualify that simply because, as I said earlier, I wouldn't expect and I don't know what kind of training you can involve yourself with other than general familiarization of prosecutors and or investigators with what a computer does.

You cannot possibly, in my estimation, hope to train an investigator or prosecutor to the extent that he knows how to program a computer or write a computer program or even understand internal logic processes of a central processing unit. You cannot do that because the only people that do that are the people working every day with computers and they don't want to be prosecutors or investigators. They want to work on computers.

So what you do when you have some information a computer crime has been committed, as I said earlier we did with an inside informant, you bring in a systems analyst or a programmer or a hardware specialist and have him tell you exactly what the methodology is and what you need to look for and what you need to track down next.

I don't think training in that regard is any more necessary than we train somebody specifically in organized crime or specifically in anti-trust investigations.

Mr. NASH. I only have one more question. Just so that the record is clear, the Colorado computer crime statute was the result of a Colorado Supreme Court decision rather than a groundswell of public support for this type of legislation, and that there was a need for this type of legislation, because there was a type of computer crime that your state was unable to prosecute under existing laws, dealing with embezzlement, larceny and fraud?

Mr. MACFARLANE. Well, I qualify that because I am not sure of all the reasons that were behind the submission of our computer crime statute.

I am aware, however, that in an analogous area, as I have suggested, that our Colorado courts, under an attempted prosecution said that the matter couldn't be prosecuted and therefore there needed to be some clarification of that with regard to our supreme court. That was at least one driving factor. Whether it was everything or not I am not prepared to say at the present time.

I think generally, however, other than that one aberration, that anything involving a computer crime, a crime involving the use of a computer could otherwise be prosecuted.

The one problem in the area is that judges, defense attorneys, prosecutors, and so forth, need to be able to visualize what a computer is. That is why I spent so much time earlier talking about it as a gigantic file system. If you visualize it as that and what a person can do with a file system with individual copies, alter them, destroy them, steal them, copy them, if those kinds of things can be prosecuted under some existing law today—and most of them can—then there should be no

problem in prosecuting a similar crime accomplished electronically. That is all I am saying.

The computer itself hasn't changed anything in terms of criminal intent and criminal act. It has simply confused people who think that somehow the computer is magic, it is a new ball game and so forth. All it does is do the same things we do ordinarily only a hell of a lot faster.

Mr. NASH. Thank you. On behalf of Senator Laxalt, I want to thank you for coming all the way out here from Colorado. We appreciate your testimony.

Mr. MACFARLANE. You are welcome.

Mr. MARKMAN. Mr. Attorney General, we have some questions from Senator Biden's office.

Ms. ZEBROWSKI. Yes, sir. Thank you very much for your testimony. Unfortunately, Senator Biden can't be here. I know he has a number of questions. With your permission, I would like to have those sent to you for your response.

Mr. MACFARLANE. I would be glad to.

Ms. ZEBROWSKI. I have a few very brief questions. Right now I know that time is running short.

First, could you briefly describe the Colorado statute?

Mr. MACFARLANE. The Colorado statute is basically the same statute with the exception of the gradation of crimes as the original Senate 240. It does not go into the extent of definitions that the original Senate 240 did. In many ways it does not need to because we are not talking about extensive Federal jurisdiction. But basically it prohibited use of computers for fraudulent purposes, or unauthorized and knowing uses, which is what the original Senate 240 did and is very close in that regard, at least in concept.

I would be certainly glad to transmit you a copy of our statute, if you would like.

Ms. ZEBROWSKI. Please. We will put that in the record, also.

[The material referred to above appears in the appendix.]

Ms. ZEBROWSKI. You mentioned that the penalties are graded based upon the amount obtained?

Mr. MACFARLANE. Yes.

Ms. ZEBROWSKI. And would—

Mr. MACFARLANE. Well, not the amount obtained, loss, damage or thing of value taken. If there is damage it would fit in the same category.

Ms. ZEBROWSKI. I realize that you don't have any experience in prosecuting under the bill as vet. Based upon the debates involved in the passage of the bill or for any other reason do you have any idea how some values might be determined?

For example, how would one determine the value of computer time if nothing is actually obtained? Say I have the computer run in my behalf and deny you access to the computer for 5 minutes. How would that fit into the misdemeanor or felony classification?

Mr. MACFARLANE. I would suggest it might possibly fit in our State law, at least, without a computer crime bill, as a malicious mischief, for instance.

Again, let me analogize. You are dependent upon a typewriter from time to time. Somebody comes and gums up your typewriter somehow

for a 3-hour period and you can't use it, and deprives you of its use during that 3-hour period. What would you do today? What is the present state of the law?

Of course, lots of things are technical violations of the law that don't get prosecuted. In terms of what you just stated in a computer framework, that 3-hour loss may or may not be critical to the user who wants to use it.

Let me use an example. I use computers in my office, as I said earlier. One of the uses I use it for is typing of documents, briefs, so forth. We have a court deadline at 5 o'clock on a given day for filing of a particular brief. If I am deprived of the use of that computer for a period of 3 hours it may be critical. I am very much disturbed and put out by it. And, in fact, it might result in some damage to somebody that I am representing because I didn't get the document filed on time and suffered some sanctions as a result. That could be very serious.

On the other hand, another use I have of the computer is to file on-line timekeeping documents. If the computer is down for 3 hours that same day and I don't get my timekeeping documents filed that day, who cares? I can get them filed the next day. Nobody is damaged as a result.

So the critical nature isn't the loss of the time so much as it is what you are dependent upon doing and what damage is caused as a result of losing that time not just the mere fact of losing it.

Ms. ZEBROWSKI. In your view then, if one were denied use of the computer for a period of time, you probably would not use this statute because that sort of offense wouldn't fall into the value-of-the-services classification. It would be very difficult to determine a misdemeanor felony. You would use another statute in that instance.

Mr. MACFARLANE. Well, what I am suggesting is that I don't think I really need the computer statute to reach the activity if it is serious enough in such a situation. I might reach it through malicious mischief or I might reach it through some other theory, but I wouldn't—whether or not I prosecute it wouldn't depend on whether or not we had a law called computer crime. It would be governed by other considerations.

Ms. ZEBROWSKI. Have you prosecuted any crimes which you would classify as computer crimes, and if so, could you very briefly summarize the sorts of crimes you are talking about?

Mr. MACFARLANE. As I say, the one instance of computer crime that my organized crime strike force has run into was an instance where someone, an internal person, a computer operator or programmer, was diddling around and got paid some money. I think it was an insurance company, as I recall, and was paying himself and some buddies of his some money on a hoked up thing, false claim.

We didn't prosecute that particular case. It was turned over to the appropriate district attorney. If I recall correctly, and I may be wrong, if I recall correctly, that person had pleaded guilty and that was before there was a law called computer crime. The plea was guilty to theft because that is what he was doing.

Ms. ZEBROWSKI. Have you had a number of cases or is this the one case that has come up?

Mr. MACFARLANE. This is the one case we have had. Now I think the Denver district attorney and maybe a few of the other metropoli-

tan district attorneys may have had some computer crimes that I don't know about.

Ms. ZEBROWSKI. When you were discussing your proposed amendments to the bill, I noticed that you didn't include financial institutions.

Mr. MACFARLANE. Correct.

Ms. ZEBROWSKI. Also, when you were discussing the future use of computers you mentioned that one's checking account may be done through home computers or telephone computers or whatever. We have previously received testimony on the future of electronic funds transfer systems and other major banking system involving computers.

By dropping out financial institutions under this statute, it is not clear that those sorts of offenses would be covered by current Federal bank robbery statutes. Do you feel that the State would be prepared to prosecute those sorts of offenses?

Mr. MACFARLANE. I am not clear first of all as to why they wouldn't be covered by Federal bank robbery statutes or just theft statutes.

Ms. ZEBROWSKI. We have some testimony and some correspondence from the Department of Justice to that effect. One of the department's reasons for encouraging the bill to cover financial institutions is their concern about the definitions of some of the terms of the bank robbery statute and whether or not under the bank robbery statute, impulses would be covered.

But, assuming they were correct, since it is perhaps arguable, could you then prosecute those offenses at the local level?

Mr. MACFARLANE. I don't see why not.

Ms. ZEBROWSKI. I do have a number of other questions, but I think we are running short on time.

Mr. MACFARLANE. I might add, I don't see why not, even without a computer crime bill at the State level. If one steals, one steals. There is sure to be a statute that covers it.

The only instance where that didn't happen was the case that I mentioned in Colorado where one copied the document and that had nothing to do with the computer, it had to do with somebody copying a hard document in a file and not taking the file out. That particular instance was not covered by our theft statute as now written. But, that had nothing to do with computers and that needed revamping. It has been done, but—

Ms. ZEBROWSKI. The name of that case is?

Mr. MACFARLANE. I am sorry. I don't have it with me at the moment.

Ms. ZEBROWSKI. Could you supply that to us then?

Mr. MACFARLANE. I certainly can, yes.

Ms. ZEBROWSKI. I do have further questions. I think we are running short on time. Thank you very much.

Mr. NASH. *People v. Home Insurance Company* is the case you are looking for.

Mr. MACFARLANE. Yes, *Home Insurance*; that's correct.

Mr. MARKMAN. We would very much like to thank you, Mr. MacFarlane. We would also like to thank the National Association of Attorneys General for sharing your expertise with us today.

Mr. MACFARLANE. Thank you.

Mr. MARKMAN. Our next witness today will be Prof. Michael Dertouzos, who is with the Laboratory for Computer Science, Massachusetts Institute of Technology.

Professor Dertouzos is the editor of a much-acclaimed book on trends in computer technology. I think he has a lot to share with us today.

Professor Dertouzos, I want to thank you for coming here. I would ask if you could perhaps summarize your testimony to the best of your ability, in light of some of the time constraints we are running into here today.

**STATEMENT OF PROF. MICHAEL DERTOUZOS, LABORATORY FOR
COMPUTER SCIENCE, MASSACHUSETTS INSTITUTE OF TECH-
NOLOGY**

Dr. DERTOUZOS. Thank you. Yes, I don't intend to take long. I would like the written testimony to be written into the record.

Mr. MARKMAN. It will be inserted into the record at the conclusion of your oral testimony.

Dr. DERTOUZOS. Thank you.

I would like to clarify that I have been asked to give my views on the future trends of computing in the next 20 years, and not to testify for or against the bill. I will indeed take that position.

It seems to me that to a great extent the legislators who are concerned with this bill ought to have a fairly good picture of the future. I am very much concerned, because there are too many people who are talking about computers, what computers can or cannot do or what computers will or will not do. Frankly, I find that I disagree or do not believe the basis on which these predictions are made.

So, this territory is a bit confused, the territory of future views, yet it seems to be very important. If I may just touch upon what one of the previous witnesses said, that the view of computers is that of giant file cabinets that one can access much faster. That is a perfectly correct view, but it is incomplete. I would like to suggest how that view might be more complete a little bit further on.

I have no assurances for the committee that my forecasts are any better than the other ones around, but I would like to tell you their basis.

The book that you referred to in your introduction is not written by me. It contains articles by some 20 of the most prominent people in the computer field, including 2 Nobel Prize winners. I am certainly basing a lot of my forecasts from that.

The other basis of my testimony is the privilege of living in a community, the MIT community, since the early 1960's, and having the benefit of electronic mail and office information and home computers for about 16 years.

So, it is on the basis of these two factors that I would like to comment.

To summarize my testimony, I have no doubt that we are at the beginning of the information revolution which I parallel to the industrial revolution, except that instead of dealing with human and animal muscle power it deals with the management and the handling of information.

The main force behind this information revolution is technological and it has to do with the established, for some 10 years now, dramatic improvement in the cost and performance of computing equipment at approximately 30 percent, per year, compounded.

This has caused tremendous decreases in the cost of equipment and has increased the prospects of the things that can be done with machines.

By way of analogy, at the forecast prices, toward the end of the century, we should be able to store perhaps 1 million characters which is the size of a large book for \$50, and a personal information base consisting of perhaps 100 books might be stored for the price of an automobile.

The more ambitious undertaking of storing the Library of Congress might cost one-half a billion dollars, at that time.

These improvements are so huge that by way of analogy if they were to happen in the automotive sector they would have resulted either at having cars toward the end of the century that cost \$10 with the same mileage that they have today, or cars that would cost then what they now cost, adjusted for inflation, of course, but that would give us 5,000 miles per gallon.

So, that gives you an idea of the drama which accompanies this information revolution.

Let me point out some of the activities that we might see and some of the applications. One of these is hidden computers. The area of hidden computers involve devices where the computer is hidden because the devices perform applications, applications of interest to their user—memo pads, special machines for dentists, for drug stores, these are the kinds of devices that I believe we will see. They will be programmed at the factory and people will not have to program them.

The second area that I would like to highlight is the area of intelligent programs which lead toward progressively increasing automation of the service sector of our economy. There are already quite a few advanced research programs in areas like clinical decisionmaking, in medicine, in mathematics, in comprehending natural language; English, for example, and so on.

By way of example, one such program that I am familiar with, a large program, is used to inform physicians of expert knowledge on the administration of a drug called digitalis, which is given for heart disease.

These programs behave very much like textbooks on digitalis, but on top of being specialist textbooks they can respond to questions from the physician as to why they recommend certain courses of action.

So, at a minimum they are a book and beyond that they can respond to questions. They have been used in actual cases in hospitals, several hundred patients, and the physicians are quite happy in using these programs as expert helpers. You understand, the relationship between the physician and the patient is still relation between humans. This is used as an intelligent text, as an advanced text that they can consult and ask questions.

There is evidence that in the balance of the century these programs are going to move into other sectors on the service side of our economy, financial services, legal services. They will be providing advice starting at low levels and moving higher up as time goes on. How high they will move we do not know.

In another automation area, factory automation and control, already we are seeing small microcomputers become very pervasive in the control of automobile systems.

During the 1980's we will see I think of all of the automobiles manufactured in the United States having at least one, up to three

computers inside them, microcomputers for safety, ignition, energy and convenience packages.

In the area of factory information of automating the factory process, the progress has been a little slower and I think it is likely to continue at a fairly slow rate. So I don't think we will see dramatic changes there.

Perhaps the biggest area is the third area of automation and I referred so far to factory information and service information. Now I would like to address office information. This I believe is the area that has already started to shoot out. That is the one where computers are going to have a maximal impact.

The scenario that we envision is with quite a high degree of certainty, the use of computers for intra-company communications and computing during the early 1980's. That means that a company like General Motors who has many plants spread throughout the United States will connect them by satellites and their companies being set up for this purpose today and will make these computers communicate with each other and pass data back and forth.

The second stage that we envision is toward the late 1980's, and that is the inter-company stage. Once these companies do have the ability to communicate among themselves it will then be natural for General Motors to want to communicate automatically with United States Steel so that it can order a part automatically without having to go through manual procedures.

We have a moderate degree of certainty for this to happen. The least degree of certainty we have for the interpersonal computer system, which, if they do take off in a big way, will probably happen toward the end of the 1980's and the beginning of the 1990's. By that I do not mean today's toy computers that one can buy, but far more capable machines that can give educational, recreational, and office type services in the home.

If these take off they probably will take off toward the middle of this period that I am forecasting, and if they do it will be very similar to citizens' band radios in that there will be a dynamics, the more of them that take off, the more they will cause to take off.

Now even with the first two factors, the intra and intercompany automation, we are going to evolve a network, an interconnected network of computers in the United States and most likely other countries of the world, as well. These networks have already begun. There are several companies that are offering network services. We will see a proliferation of these, and of this I am quite certain, in the years to come.

It is in this area of interconnected computers with communications that I think the biggest difference rests between today's and the past computer systems. Perhaps now I can come back to the analogy of the giant file cabinets.

The proper picture as I see it in the future is indeed giant file cabinets, many of them, and many companies, interconnected with subterranean pipes through which agents, and I mean the term "agents" in an abstract sense, programs, messages, can flow, can pose requests, search in the file cabinets, if the protective systems are not adequate and transport information back and forth.

In other words, a significant difference between the interconnected computer systems of the future and today's offices.

One of the biggest fears that I have from that scenario is that machines, computers themselves can be used to conduct such unauthorized expeditions into the data possessed by other machines. It is possible for an experienced programmer, in the absence of appropriate safeguards, to construct programs that will go searching around for a long time trying to build up whatever is desired to be built up and leaving no trace.

So, perhaps giant file cabinets connected by subterranean pipes where it is possible that no traces are left is the more accurate picture in my own view.

I have listed in my testimony, and I do not want to repeat now, several positive and negative socioeconomic consequences that we expect are to the proliferation of computers.

There is no doubt in my mind that computers will become more and more pervasive as time goes on and that they will become a very important factor in our everyday use.

So, instead of repeating these positive and negative factors which are summarized in any event in the testimony, I would like to focus on one last item, if I may, since I have the attention of some legislators. I would like to call attention to what I see as a possibly unprepared state that we may be in. The information networking that I discussed earlier which we occasionally call the information marketplace of the future where companies and individuals through their computers and communications equipment are interconnected and buy and sell services and information from each other.

In this view, I am very much concerned that a sizable investment, tech-economic investment, will have been made by the time we recognize legal problems that such an interconnected information marketplace may create. I would very much like to hope that the very able legal minds that are capable of coping with this matter pay attention to it thoroughly before we have made this irreversible tech-economic assessment.

Let me cite some of the questions that to a lay person in terms of law, such as myself, come to mind.

One: The extent to which information should be or should not be treated like real property.

Two: The extent to which programs should be protected from unauthorized duplication and misuse.

Three: The regulation of computer-to-computer interconnection. Let me just pause on that and give a very quick example.

Is it, for example, necessary in the future, before two giant data bases, belonging to different companies, different organizations, before such two data bases become interconnected, is it desirable that they demonstrate a certain standard of safeguarding which will prohibit these subterranean pipes that I discussed earlier from collecting and aggregating information between these two data bases, or is that not necessary from a legal point of view.

Let me move on.

Four: The desirability for mandatory audit trails whenever sensitive information is read or changed by anyone. Is it desirable to have

mechanisms and techniques that will leave permanent trails if someone plays with such interconnections.

Five: The desirability for mandatory destruction of machine-store information after a certain time has elapsed, and I don't mean this strictly in the sense of privacy where we already have some established legislation.

Six: The development of criteria for what kinds of information may not be stored in machine accessible form.

Seven: The handling of authentication violations.

There is a very significant new issue that will crop up which I refer to as authentication in which the purported signatory of a computer message is an impostor and how does one cope with that.

Eight: The regulation of unauthorized expeditions, and I mentioned this earlier, typically aided by either computers over data bases, and knowing the purpose for confusion of mistakes with planned computer crimes in badly organized machine installations.

If machine installations in fact are allowed to move without any standards for any regulations, then might there not be a purpose for confusion of mistakes with a crime.

Well, with this I would like to observe that once again the information revolution is upon us. The growth of computers is and will continue to be pervasive throughout the next two decades, I believe. Information will become indeed, and its management will become indeed a major factor in our way of life.

Thank you.

Mr. MARKMAN. Thank you, professor.

Your written testimony raises some very intriguing questions, some of which you have touched upon very briefly here today.

I have just two questions I would like to ask you, if I could very briefly.

Dr. DERTOUZOS. Yes.

Mr. MARKMAN. First of all, do you see any personal privacy implications in S. 240? I believe you touched upon this very briefly in your written testimony. Do you see any personal privacy implications in the centralization of responsibility for computer crimes in a single governmental jurisdiction, that is, the Federal Government?

Dr. DERTOUZOS. Indeed, I do. In fact, in my write up, I do make the point that in nondemocratic countries it is likely. In fact, I have evidence that there is a movement to a computerize centrally a tremendous amount of data concerning the travel of individuals and information about whereabouts and additional information.

In our society, this is not as likely because of the many checks and balances that we have. But whenever any agency, however benevolent it may be, is in control or is capable of controlling massive data about individuals then the prospects for violation of privacy is there.

Indeed, I would like to see substantial safeguards that will insure that this will not be the case.

Mr. MARKMAN. Is that possible, do you think, in the context of present technology?

Dr. DERTOUZOS. Technically it is beginning to be possible now. There are new techniques that have been recently developed that make safeguarding of data bases and communications quite feasible. I think

these techniques will evolve in even better ways in the future, but—the answer is technically, yes. That would be the quick answer. But the crucial answer is not there. It is on what will motivate people to install such techniques in the absence of guidelines or regulatory legislation.

Mr. MARKMAN. Let me ask you one other thing. Without asking you to make any value judgments of your own, but conceding for the moment that there are a number of Senators on this committee who are concerned about preserving roughly the balance between State and Federal jurisdiction that presently exists today, what would be your views with respect to the concern these people have about this legislation?

Do you see this legislation extending Federal jurisdiction as computer technology grows more pervasive?

Dr. DERTOUZOS. As I said earlier, I am not prepared to testify for or against the bill. I frankly see this legislation as very inadequate and tackling a very small portion of what I see as a major problem in the future. I am not necessarily implying that we need more regulation, but we need more good, legal minds thinking about this problem now. So, I guess I do not have a comment for you on that.

Mr. MARKMAN. Thank you.

Mr. NASH. Professor Dertouzos, when you stated that in the next 20 years we are going to have a 256-fold increase in computer storage capability, how does that grow from a base of where computers are at 1 now?

Dr. DERTOUZOS. Yes.

Mr. NASH. How does that grow from 1 to 256 in the next 20 years?

Dr. DERTOUZOS. Well, that is what you get if you have something between 20 and 40 percent per year, compounded.

Mr. NASH. So, that being the case, that computer capability is going to grow quicker and quicker every year. Is it possible to legislate to keep up with that type of a progression?

Mr. DERTOUZOS. Well, I am not really familiar with the capabilities and limitations of our legislative bodies, but I would think that educated people with basic understanding of science can comprehend the issues that are coming ahead and can prepare for them in the way they think is best.

So, I guess I am an optimist on this. I think we can. I would like to see us be prepared before the irreversible commitments have been made which I see happening every day in our capital investment of companies making investments in installations, interconnections of installations. We may just wake up one day and discover that we should have thought about this earlier. That is really all I am calling for.

Mr. NASH. In your statement you spoke of a possible future scenario where a computer would "wake up" if 10 people that were being monitored appeared in the same city at the same time and that would only be possible, I suppose, if you had these rather extensive network services that you talked about.

Dr. DERTOUZOS. Yes.

Mr. NASH. Is that essentially where you have to look if you are going to regulate and if you were going to look there to regulate, would that stop that almost geometric growth in computer power 20 years from now?

Dr. DERTOUZOS. Well, I think you can isolate to some extent the growth from the uses of the growth and the equipment. That example that I brought up which is if you asked me today to write a program that wakes up whenever 10 people of a designated political group meet in any U.S. city, I would say that is very difficult to do today and costs a great deal in terms of resources, money, people, time, et cetera. I suppose it could be done somewhat with a vast army of detectives, but it would be very difficult because the data bases containing this information are spread throughout hotel managements and travel—airline travel reservations and so on and other records.

But in a future society which in the scenario, the interconnected information marketplace where all this data is indeed stored in machine form somewhere, if indeed it is possible to crawl around in this space of machines and acquire and pose questions by another program that collects this information, without safeguards in the interconnections, then you can have this problem.

It seems to me that if we wake up one day and realize that this is possible and now there is an invested base of \$100 or \$200 billion of equipment that is interconnected, it would be very difficult to pose at that time the kind of actions that we would have taken had we thought about this earlier.

Mr. NASH. I know that when you are even at this level working with the bill that we have before us, S. 240, that essentially deals with computer fraud, you run into absolute roadblocks when you try to define "computer" for use in the legislation.

Dr. DERTOUZOS. I think it was very good up until recently when computers could be enclosed in one room or one giant warehouse. Now that they are becoming blended with communications networks, the place where the computer stops and the communication network starts is becoming more and more hazier, and in fact, it is becoming a more difficult problem. In fact, some of the networks that are being planned by the common carriers have an intense computer component in them.

It is very difficult to tell when you have such a giant network, computers and communications, where one starts and where the other one stops.

Mr. NASH. Thank you.

Mr. MARKMAN. Senator Biden's office.

Ms. ZEBROWSKI. Thank you.

Your testimony has been interesting. I have a few brief questions. It has been suggested that enacting Federal legislation may have the impact of stifling creativity by programmers and others in the field who fear that their so-called experimental activities may result in their committing an offense of any sort, and that even discussions of developing legislation or discussions of developing regulations stifle such creativity.

Do you have any insight into whether or not that is true?

Dr. DERTOUZOS. Well, I am sure that in some general sense that is true. Any kind of constrictive and restrictive activity does stifle the creativity of the human brain. But we do have regulatory activities in other areas. When we enter a giant wide-bodied airplane we do have certain assurances that somebody has worried about our safety.

In that sense, our creativity in designing aircraft has not been reduced or in designing transportation systems, at least to my knowledge.

I think within some kind of a balanced framework—I am not an advocate of Government regulation, increased regulation. Quite the contrary. I am just alerting the committee to what I see as a major factor in the future and I don't see many people worrying about this factor.

I think a balance can be stricken between regulation and freedom.

Ms. ZEBROWSKI. You describe a future where we are increasingly dependent on computers. They will process sensitive, private, and important financial information for individuals and for corporations and the Government. What do you see as the potential impact of any sort of damage to such computers? Can you hypothesize on what that might result in?

Dr. DERTOUZOS. You mean what kind of damage this might cause upon us?

Ms. ZEBROWSKI. If a crime perpetrated on the computer results in damaging the computer or the system or the software.

Dr. DERTOUZOS. Oh. I see. Then what might happen?

Ms. ZEBROWSKI. What might be the result?

Dr. DERTOUZOS. Well, I think this is an area that again, we have to be very careful. If there are computers that are being relied upon very heavily, for example, in medicine or in safety, in our safety, and these computers do malfunction, we may be lulled into having undue trust and responsibility in these machines. I have confidence that we will not, that the people who are involved will try for safeguards. But, as we are embarking in these new areas, in these new territories, as we saw in Three Mile Island, it may be difficult to predict ahead of time what some of these problems may be.

Ms. ZEBROWSKI. It could then have a tremendous impact on private industry.

Dr. DERTOUZOS. Absolutely. If one were today to destroy the airlines reservation data banks of a major airline that would cause, I believe, very, very far-reaching repercussions.

Ms. ZEBROWSKI. Do you have any insight into the ease of detecting, investigating and proving misuse of computers?

Dr. DERTOUZOS. It is very difficult to do so today because it is possible for programers, experienced programers and other people, and I am a programer myself, so I speak with some experience, to make changes in computer systems without leaving traces.

So, in the absence of any enforceable traces or mechanisms thereof, it is not very easy to detect.

Ms. ZEBROWSKI. What about after it is known that a crime is going on, how difficult is investigating that crime and proving the fact that it occurred?

Dr. DERTOUZOS. That is a terribly complex question. I don't think that I could answer you responsibly. I think there is a lot to be said in that area. I would like to think more about it.

Ms. ZEBROWSKI. Would it be possible for you to respond in writing at some later time?

Dr. DERTOUZOS. If you would sharpen your question a little more.

Ms. ZEBROWSKI. You mentioned that programers can now search other programs, not theirs, and not leave a trace. Are there any other sorts of activities along those lines that you see going on now?

Dr. DERTOUZOS. I am sorry. I didn't say programers are doing that. I said it is possible in principle to do things of that kind. Most of the programers I know are very moral people, like other people.

Are there other activities you mean, of the same kind that could cause computer crimes?

Ms. ZEBROWSKI. Yes.

Dr. DERTOUZOS. Again, I think this is something that I could list for you. I could give you a list of possible activities, yes. Not now. I would like to do it later.

Ms. ZEBROWSKI. Thank you very much.

Mr. MARKMAN. Professor Dertouzos, I just have one other matter that I would like to ask you about. You indicated that there was increasingly developing a blend between computer technology and basic communications media.

Dr. DERTOUZOS. Yes, sir.

Mr. MARKMAN. I am just thinking aloud, perhaps, but do you see any possible first amendment implications in what we are doing here, any question, perhaps, that ought to be explored in this area?

Dr. DERTOUZOS. Yes. Precisely. That is the reason I would like to alert the committee to do some deeper thinking with the people who are experienced in these areas.

Mr. MARKMAN. We very much appreciate your taking your time to be here today. Your written testimony in particular will be invaluable to the members of the committee.

Dr. DERTOUZOS. Thank you.

Mr. MARKMAN. Thank you very much, Professor Dertouzos.

[The prepared statement of Dr. Dertouzos follows:]

1. PREFACE

This writeup addresses the question "How might computers develop in the next twenty years and what might their impact be on our society?". The question has been posed by the Staff of the U.S. Senate Judiciary Committee in connection with hearings on Bill S.240, The Federal Computer Systems Protection Act of 1979.

2. INTRODUCTION

There is by now little doubt that we are the first human generation of the Information Revolution. This movement can be likened to the Industrial Revolution, except for its focus on the mechanization of mental-informational rather than muscular-physical activities. Faithful to this analogy, the Information Revolution has its roots in technological innovation and its promised fruit in the socio-economic structure of the world.

Today's technological predictions about the future course of the Information Revolution vary widely: Visions of intelligent robots that may even decide to dominate us some day are tempered by difficult technical problems and by the slow progress of today's mundane programs and machines. There is also considerable conflict among knowledgeable scientists as to how far along the ladder of intelligence computers may eventually ascend. Similarly, the automation of educational, medical, recreational and other services, as well as the automation of factories and of offices are simultaneously heralded and downplayed by different forecasters. Finally, the prospect of computers in the home is the subject of much speculation and emotional controversy. These widely varying technological projections are accompanied by even more uncertain predictions on the impact of the Information Revolution on our society: Optimistic visions of an improved and more productive life are presented side by side with forecasts of our eventual dehumanization.

This writeup summarizes the author's views on some expected technological developments and socio-economic consequences of the Information Revolution. While it is based in part on a recent book* and on current computer science research, it is ultimately the product of the author's imagination and personal bias.

* M. L. Dertouzos and J. Moses The Computer Age: A Twenty-Year View. MIT Press, 1979.

3. SOME EXPECTED TECHNOLOGICAL DEVELOPMENTS

3.1. The Hardware and Software Base

The main force driving the Information Revolution is a steady improvement of some 30% per year in performance/cost and size/cost of primary solid-state memories and processor components. This improvement which has been going on for over ten years is expected to continue well into the 1980's and early 1990's. By the end of this century a 256-fold improvement is likely relative to today, leading to a cost of perhaps \$50 for storing one million characters. This, in turn, means that a personal information base equivalent to 100 books may be stored for the price of an automobile. The far more ambitious undertaking of storing the world's written knowledge would still be very expensive but not prohibitive at about one half billion dollars per LOC*.

These expected hardware improvements are so huge that were they to happen in the field of personal transportation, they would promise by analogy a future price of \$10 for today's cars or a future fuel efficiency of 5,000 miles/gallon at today's car prices.

Unlike the spectacular performance/cost improvement of the hardware, the process of developing programs for new applications continues to be not only very costly but a progressively increasing fraction (typically over 50%) of a computer system's total cost.

To my thinking, the most promising prospects for reducing software costs rest on two developments -- hidden computers and intelligent programs -- discussed respectively in the following two sections.

* The LOC (for Library Of Congress) unit of memory was established half jokingly, half seriously by the author to represent large amounts of information.

3.2. Hidden Computers

Programming a computer is a consequence of an historic relic -- the effective utilization of a scarce and expensive resource. In the early days of the field, when computers used to cost a great deal of money, it was natural that different users prepare their programs and wait in line for hours, if not days, to get a few minutes of the computer's valuable time. Later, when time sharing came into wide-spread use, programmers still had to program in order to time share the still expensive central resource. With future computer costs converging to zero, this is no longer a valid reason for programming. Instead, a program can be developed at the factory, converted to hardware and then sold in large quantities with the computer thrown in at little or no extra cost. Such systems dedicated to individual applications will no longer be viewed as computers to be programmed but rather as appliances that perform specific tasks -- hence the name "hidden computers". Hidden computers offer an economic solution to the high cost of programming since that cost is spread over a large number of users.

We might then see in the balance of this century machines such as the memo pad, carried on one's person and capable of storing away and retrieving information of personal interest; or the drugstore machine, which replaces the cash register and takes care of the inventory maintenance and reporting needs of a small business; or the dentist machine, that keeps appointments and handles billing for dentists, or the secretary that keeps a list of up-to-date addresses and phone numbers and helps process memos.

3.3. Intelligent Programs and Service Automation

Today's research programs that are characterized as "intelligent" exhibit expertise in such diverse fields as clinical decision making, mathematics and circuit design. Take for example a recent program developed at the MIT Laboratory for Computer Science that tries to behave like an expert physician in the administration of the drug Digitalis. Given the patient's history and symptoms, this program recommends appropriate dosage amounts. The program contains within it a good deal of knowledge about Digitalis, much like a book on that subject. Unlike a book, however, the program can respond to a non-specialist physician's questions. Matching human queries to

machine explanations is one of several features that distinguish such knowledge based (or intelligent) programs from specialist texts.

Features such as the above, along with other capabilities and on-going improvements suggest the future use of knowledge based programs for the automation of services. Indeed it is not too far fetched to extrapolate the behavior of early research experiments to programs that help in the dispensation of educational, legal, recreational, financial, governmental and business services. The automation of certain services by computer further suggests as a major potential advantage the tailoring of services to individual needs -- an activity that is also possible with manufactured goods, as we discuss in the following section.

3.4. Factory Automation

In applications of control, instrumentation and factory automation, it is already evident that inexpensive Micro-computers are displacing traditional control and instrumentation systems because of their flexibility to follow different strategies, their ability to communicate with other processors, and their low cost. Such systems have already appeared in automobiles (cruise control, ignition control), in aircraft and ships (navigation computers) and in factories (process control). Many others are now at the design stage, for example emission control and safety computer systems that will soon appear on board automobiles.

Beyond traditional control and instrumentation lies the science fiction writers' workhorse -- the robot. General-purpose robots that can be programmed to perform different tasks have been in existence for some time, e.g. in the welding of automobile frames. Such robots, however, behave like "tape-recorders", in that they mimic exactly a preset motion. Of far greater interest are robots capable of sensing their environment especially through vision, and adjusting their motion to suit what they see. Early research experiments with such robots have established the not so surprising conclusion that the greatest technical difficulty lies in perception -- that is, in understanding a scene, sufficiently in order to act upon the work pictured in the scene. Accordingly, progress in such programmable general-purpose robots is dependent on progress in computer vision. Progress in that area, in turn, has not been very promising. In the future, a breakthrough in machine vision may take place if we can

successfully harness multiple (perhaps 1000 or more) processors to the task of visual perception. The coordinated use of many inexpensive processors may be extended to other domains as well, such as speech recognition, thereby opening up major potential applications in a new field -- Sensory Computing.

Regardless, however, of the progress in sophisticated robots, we may very well see applications of computers to factory automation through less sophisticated sensing (e.g. tactile) techniques, and through special-purpose assembly-line computers. The latter will monitor and control the manufacturing process, and by communicating with each other and with higher-level "planning" computers will tend to increase manufacturing productivity.

The most exciting prospect in this area, however, is the potential for tailor fitting of products to individual needs. The computer is eminently suited to such mass individualized production, as for example, in the manufacture of apparel, furniture, and other products whose size or function is adaptable to varying human needs.

3.5. Office Automation

Of the three potential areas for automation -- service, factory and office -- it is the latter that is most likely to exhibit the fastest growth. The reason lies in the coincidence of strong supply and demand forces for a new office technology. On the demand side, office workers continue to be under-capitalized and to rely on minor improvements in capital equipment. At the same time, they are confronted with increasingly complex information management requirements and rising productivity expectations. On the supply side, the decreasing computer hardware costs and the availability of reliable and low-cost means of communication form a foundation for growth of a new office technology.

This technology is likely to lead (in order of increasing technological difficulty) to (1) word processing and text formatting; (2) low-cost transmission of mail and messages (data, voice and still images); (3) automated intra-company office procedures; (4) automated inter-company business transactions; (5) sophisticated filing and retrieval of information; and (6) evolution of the so-called information marketplace.

The first two of the above developments are self explanatory. Intra-company office automation pertains to such activities as forms management, the processing of messages and the formalization of certain office procedures. With the advent of satellite communications, intra-company automation of geographically dispersed offices will come of age -- perhaps by the mid 1980's.

Inter-company office automation is organizationally and technically more difficult than its intra-company equivalent because it involves interaction among a number of different and autonomous organizations. The organizational problems involve such issues as the need for common inter-company communication conventions and business transaction standards. The technical problems are associated with the interconnection of thousands, and later perhaps hundreds of thousands if not millions, of cooperating computer ports such as terminals, small personal computers, and larger communal machines. Significantly, these machines will not be under centralized control, as is the case with almost all computer systems that have been developed to date. Accordingly, we do not yet know how technically difficult or easy their effective inter-connection will be. These systems are envisioned as being decentralized, large, and complex interconnected aggregates.

We turn next to the prospects for more sophisticated filing and retrieval of information. In spite of much recent fanfare surrounding data bases and data base languages, the problems of filing and retrieving information effectively continue to be substantial. One common problem is the aging of data and the progressive inconsistencies that plague current data bases. A far more serious problem, however, is the limitation of today's data bases to answering only queries that were anticipated by the data base designers. The far more useful prospect of organizing incoming data in such a way that it can be retrieved when a relevant, but unknown-at-filing-time query arrives is still largely unsolved. The prospects for such sophisticated

filing and retrieval systems are not clear at this time. They are necessary, and are sure to revolutionize office technology if and when they arrive.

Finally, my forecast of an information marketplace refers to the environment that will be created by large numbers of interconnected computer ports. In particular, as these ports increase in number and in the wealth of offered and consumed services, they will give rise to a free market where information can be traded as if it were a commodity.

3.6. Home Computers

We can buy today "toy" computers typically without intercommunication capabilities, that are barely beyond the level of a desk calculator and typically offer some entertaining games and a minimal programming capability. It is possible, however, that these machines are the awkward predecessors of tomorrow's widely used personal computers. The latter are expected to provide educational, recreational, medical, financial and other services primarily through their interconnection with the information marketplace, and secondarily through packaged locally contained programs. These machines are also expected to maintain a wealth of personal information, make possible electronic mail, and link the office to the home.

Even though the economics for achieving such home computers are realistic, ultimate developments will depend, as in the case of CB radio, on the dynamics of home-computer users. This is the case because the real utility of such systems hinges on communications and the existence of a large number of interconnected suppliers and consumers of information. We are therefore led to the conclusion that inter-personal information systems, if they materialize, will follow intra- and inter-company computer applications sometime in the late 1980's or early 1990's. Were such developments to happen, however, they would lead to a massive growth of the information marketplace and to profound effects on our way of life.

4. SOME EXPECTED SOCIO-ECONOMIC CONSEQUENCES

Some commonly cited* negative factors on the impact of computers on our society are as follows:

1. **Superior Machine Intelligence:** Knowledge based programs become so intelligent as to be threatening to humans.

2. **Human Displacement:** Continuing progress in office-, service-, and factory-automation will result in the displacement of human labor from the corresponding economic sectors.

3. **Dehumanization:** Increased computer acculturation of our society will cause progressive suppression of traditional values and will promote a narrower technologically based thinking mode.

4. **Mental Atrophy:** This is a likely consequence of the information revolution in the same sense that the industrial revolution decreased the need for and capability of human and animal musclepower.

5. **Undue Trust of Machines:** People may be intimidated into courses of action they do not understand, because of undue trust on computer generated plans and advice.

6. **Responsibility and Liability:** Large programs developed by many authors tend to diffuse responsibility of authorship. Who is responsible when such programs malfunction and cause us harm?

7. **Reduced Privacy and Computer Crime:** Aggregation of information about humans in machine form and intercommunication of sensitive information among computer systems offers many possibilities for abuse.

*An excellent treatise of these and other problems appears in J. Weizenbaum, Computer Power and Human Reason

On the issue of superior machine intelligence we have no scientific basis today to assert that computers will either reach or not reach our level of intelligence in the future.

Some human displacement by machines is likely, yet at a slow rate and over a period of several generations. To start with, there are some human jobs for which machines are better suited than humans, such as work in hazardous environments. Then there are highly repetitive assembly-line jobs that are certainly not contributing to our humanization -- they are likely to be gradually taken over by machines. Regardless, however, of the types of jobs that will be replaced by machines, we should feel no more and no less threatened by such events than by the earlier displacement of people from certain jobs as a consequence of the Industrial Revolution. If such a transition is slow; if it replaces lower-level functions and if it spans several human generations, as seems to be the case with the Information Revolution, then the human labor force is gradually displaced toward more challenging and less mundane activities.

In the area of de-humanization we often hear about our potential de-humanization, without stopping to consider that we have been already considerably de-humanized through the Industrial Revolution. Gone are the artisans and craftsmen of the pre-industrial era with their tailor-fitting products and services. The low-cost, mass-produced goods and services of today have reduced us to affordable uniformity and impersonal numerical identities. To my thinking, the much feared computerization of our society may indeed if not reverse, at least balance some of these de-humanizing trends -- in particular, it may make possible through factory-, service- and office-automation the tailoring of goods and services to the most variable of demand centers, ourselves -- at affordable costs. This mass individualized production may indeed be one of the most important consequences of the Information Revolution.

I have no doubt that some mental atrophy will accompany the information revolution as and if knowledge based programs become more capable. It has already started in arithmetic with the advent of the inexpensive calculator. This is clearly an area which we should watch with caution and try to anticipate through control of our educational system.

Undue trust is placed on machines by some people who are

either unaware of a machine's capabilities or who purposefully wish to deflect the opinions of others. While such cases will undoubtedly arise, it is my belief that they will not be frequent, since people will seek to comprehend and question the results of computing machines as they have done for other complex machines. This issue is linked with the question of responsibility and liability. I cannot conceive, for example, of a physician who will install and use a program on digitalis therapy without comprehending how the program works and without identifying a human organization that is accountable for the program's actions.

The most important concern that I have about the societal consequences of computers involves the prospects of reduced privacy and related computer crimes. This issue, in turn, is linked to a techno-economic issue -- the extent to which future computer resources will be centralized or decentralized. Where such resources are centralized, it is inevitable that information pertaining to us will be aggregated, correlated and ultimately misused. Even if a benign organization has centralized control of such information, the information may eventually come into the wrong hands at the wrong moment. Consider for example the imaginary case of a political leader who asks today for a program that "wakes up" whenever 10 or more people of a given political group meet in any U.S. city. Such a task cannot be easily pursued today, simply because the information needed by the program is either unknown, or distributed among many independent organizations in the form of airline manifests, credit cards, hotel registration forms and so forth. If all of these databases, however, were mechanized under one central authority, then they could be easily searched by computer. It is this last factor of easily reachable information by machine that makes privacy and other computer crimes a dominant issue in the Information Revolution.

While in the U.S. and other democratic societies, centralization of information is unlikely, the opposite holds true for autocratic centrally controlled political systems, which, by their very nature, are likely to make sizeable investments in centralized installations. Fortunately, the pluralistic and heterarchical information marketplace that we forecast is no more centrally controlled than the marketplace for goods and services -- a bright prospect for the future of privacy in democratic societies. In this area, it is the obligation of the citizenry and of the government to maintain active vigilance toward potential privacy violations and to provide safeguards for

avoiding such violations in the first place.

In spite of the reduced prospects for centrally directed violations in systems with distributed authority, such violations are possible surreptitiously and may even be easy, because of the presence of interconnections among many computers where information is stored. Fortunately, the technology for safeguarding information among interconnected computers is progressing well -- It is therefore likely that by the turn of this century we will be able to provide adequate safeguards for interconnected and autonomous computer systems. Meanwhile, we have an obligation to insure that before any data bases become linked to one another, enough privacy safeguards are introduced to make the prospect of potential violations tolerable. In the absence of such demonstrable safeguards, our responsibility is clearly in slowing down or arresting, most probably through regulatory means, such interconnections.

Ultimately, of course, computer crimes are, and will be, perpetrated by people and not by machines. What is significant about computer abuses of the future is that they will likely be novel, easier to commit and harder to detect, precisely because of the dramatic growth of the computer field. To strike a proper balance between individual freedom and tolerable regulation will surely be a substantial legislative and judicial challenge.

To my thinking, it is important that we pursue major and comprehensive information-related legislation soon since by the time such legislation becomes unavoidable, we may be well into the information marketplace era with a sizeable and irreversible techno-economic investment behind us. Some issues for consideration by such legislation beyond privacy violations and financial computer crimes include: (1) the extent to which information should be treated like or unlike real property; (2) the extent to which programs should be protected from unauthorized duplication and mis-use; (3) the regulation of computer-to-computer interconnections; (4) the desirability for mandatory audit trails whenever sensitive information is read or changed by anyone; (5) the desirability for mandatory destruction of machine stored information after a certain time has elapsed or other conditions are met; (6) the development of criteria for what kinds of information may not be stored in machine accessible form; (7) the handling of authentication violations (when the purported signatory of a computer message is an imposter); (8) the

regulation of unauthorized expeditions (typically aided by other computers) over data bases; and (9) the purposeful confusion of "mistakes" with planned computer crimes in badly organized machine installations.

Moving away from negative factors we summarize next the potential benefits of the Information Revolution as follows:

1. **Increased productivity through automation of services and through factory and office automation**

2. **Reduced Energy Dependence through replacement of current energy consuming activities e.g. transportation of people by transportation of data.**

3. **Tailor-fitting of Products and Services** We have already discussed the prospects for mass-individualized products such as apparel or services such as individualized newspapers and advertising -- at mass production costs.

4. **Information filtering** This refers to the selection, by machine, of information important to us, and the screening away of the ever increasing amounts of informational junk.

5. **Improving our way of life:** Through increased convenience through the availability of useful service and through liberation of minds in tackling un-interesting, repetitive and generally mundane tasks.

6. **Augmenting the Labor Force:** by making possible through the information marketplace the employment in information services of rural people, of handicapped individuals, of care-takers of small children and in general of people who cannot physically leave their home.

These benefits need not be further discussed here, as was done with the earlier negative factors, since as is by now clear this is the writeup of a technological optimist who does not plan to argue against his own position.

Let us observe, instead, that information -- unlike food, shelter, health, or energy, is not a primary factor to human survival. It is, however, necessary immediately after these basic factors, for it helps us plan and carry out actions aimed at satisfying our most basic necessities. It is my view that in this role, as an important, but non-vital necessity, information and its management by the Information Revolution, will contribute to human progress, and will find its proper balance within human endeavor as did its pre-cursor -- Industrial Revolution.

Mr. MARKMAN. The next witness will be Mr. John K. Taber, a professional computer programmer from California. Mr. Taber is also the author of numerous articles on computer crime legislation. He has commented at some length about Senate bill 240 for the past several years.

I would like to thank you very much for coming today, Mr. Taber. I invite you to summarize your testimony as well, if you could. We would like to ask you just a few questions afterward.

**STATEMENT OF JOHN K. TABER, PROGRAMER,
SANTA CLARA, CALIF.**

Mr. TABER. I will try to be as brief as possible.

My name is John K. Taber. I am a computer programmer. I want to emphasize that I am speaking strictly as a private person.

I don't represent any organization or any other person. My interest in this bill was originally aroused by the language which had "unauthorized access," and I realize that myself and many other programmers make what we might call the unauthorized access of the computer. I was very concerned that they would be technically felons.

The subcommittee has done a very good job in cleaning up the language of the bill so I no longer feel that is a problem; unauthorized access has been completely dropped from the bill, which I think is very good.

I do think that it still needs a misdemeanor provision, but apart from that I don't think that it would pose problems for programmers or for the data processing community with the bill as it has been revised.

But I am still not enthusiastic. I feel that the bill is unnecessary, first, because in my research into computer crime I find that it is an insignificant problem.

Second, I do believe that existing criminal law is adequate to cover what problems do exist.

I would like to say that I think there is a widespread impression that computer crime is a growing and serious problem. I think that that is a misrepresentation that is due to misinformation in the media.

I have an example—the very first computer crime story of which I am aware—which occurred in the Wall Street Journal, in April 1968. It essentially recounted three computer crimes. It turned out two of them occurred before the firms even had computers. It is this sort of inaccuracy that we are constantly battling.

As it turns out, that was really pretty good journalism, pretty good accuracy for newspapers because I have encountered crimes in the newspapers that were so fantastically distorted that you could not get the facts.

In going through studies of computer crime I tend to take a very strict definition of what should be a computer crime. I define computer crime as something where a computer is directly and significantly an instrument of a crime. I don't believe that if you forge a credit card receipt that that should constitute a computer crime.

From a very strict definition of what should be a computer crime so far I have encountered two cases. One was a programmer in Minneapolis who had installed the banking check handling system and he pro-

gramed it so that it would ignore overdrafts on his own account. When he was caught he was \$1,357 overdrawn.

The second computer crime which I think is a genuine crime concerns the Flagler Dog Track theft which involved actually stopping a minicomputer, I suppose by an abstop mechanism, and changing the totals of the winners and the losers in storage and then allowing it to run through to completion.

It turned out that the investigator, once he was assigned to the case, he was assigned to it quite late, was able to—my understanding is was able to solve how it was done and everything within 3 days. The only real problem that he had was the time constraint because when he got assigned to the case the season was over, was going to be over the next day.

I mention that because I think that there has been a lot of inaccuracies in how difficult it would be to prosecute a computer crime. I don't see any difficulty in the cases that have really happened.

I also mention and emphasize these two real cases because in testimony here and in supporting documentation provided to Senator Ribicoff's committee there were several fictitious computer crimes. There is a number of mythical computer crimes which is widely believed. They were cited in testimony, but they simply are not true. They are apocryphal cases. They arise in folklore.

Also, there have been a number of crimes which have been called computer crime but never involved the computer even in the remotest way. These again were cited in testimony here and in fact even quoted by the Senator.

But there are a bunch of crimes, although I don't think as many as many people believe, which I would call bookkeeping crimes. These are in cases where somebody, like the credit card receipt case or one of the cases in Colorado which the first witness was apparently unaware of where somebody working in a stock brokerage firm changed some stock codes so that he could borrow money on a stock that wasn't suitable for a margin account. This was done entirely by manual means. He did it by changing the forms and then they eventually wind up in key punch or in data entry and entered the computer that way.

I really don't call these computer crimes, but you know I don't know if it is important to argue it. It just seems to me that this is a normal theft or fraud or forgery case.

Trying to count how many of these cases the GAO found, 69 cases, and by the way, I would like to correct something. The first witness quoted me and I had said there were actually 66 cases. It turns out that I was mistaken. There really are 69 cases. I had doubled counted three cases accidentally. But this was throughout the Federal Government. I had called Walter Anderson on this and asked him to try to get an idea how thorough a search this was. My impression is that it was a pretty thorough search. Now it is always open to question how thorough, but my impression is that it was a fairly thorough search.

I emphasize the 69 cases as an insignificant amount.

SRI has been investigating cases. He claims 633 cases of computer abuse very recently.

But I have to emphasize that Parker's computer abuse should not be confused with computer crime. He has many cases in there that have

nothing to do with crime. He has many cases in there that should not be made. He has some cases in there that don't even involve computers.

It is kind of confusing because he is studying many different things besides crime.

Parker estimated that there were \$300 million a year in loss into computer crime currently. I question that figure. I think that it is made without justification, but even if you accept it, the U.S. Chamber of Commerce estimates a total loss of \$40 billion a year, not for computer crime, but for white collar crime in general.

If you do the arithmetic, computer crime even used in Parker's figure, is three-quarters of 1 percent.

I am trying to emphasize that computer crime is a rare and insignificant problem.

There is conflicting evidence. The American Bankers Association, in 1978, conducted a survey of automatic teller machine operations. What they found was that automated systems were safer than paper based manual systems. Losses were either nonexistent or when they did occur were less than in manual systems.

In the few cases when loss did occur, the average loss was \$20. Now this is completely contradictory of the exaggerated loss figures claimed by Evers.

There was an earlier report in 1972, a study of internal frauds in banks, by the Bank Administration Institute. They said in no case of bank fraud was the computer instrumental.

In other words, bankers have repeatedly claimed that they do not have the security problem with automated systems.

I don't know if there are any other studies comparable to the bankers for businesses in general, but I think that it would have the same results because the fact is computer crime is not easy to commit.

I know that the Senate has been told that a programmer could easily commit such a crime. That is not true. Now I don't mean to say that to commit a crime is impossible, but practically speaking, it is quite difficult.

The fact is that records are now magnetic blips. They can't be detected without machinery and really an enormous amount of programming. The programming is complex and difficult. This automation curtails the number of people who can get at the books.

In contrast, before you had computers, you had an office building full of clerks. Any one of them could have gotten at the books and they would be capable of doing so if they wanted to commit a crime.

The number of people capable of committing a crime now are greatly restricted. Of course, we talk about bookkeeping crime.

Furthermore, the computer has tremendously increased the powers of management to audit, to control their books and assets. Before computers it would have been very difficult to check to validity of every account even in a medium sized bank. With computers I think that can be done routinely, even in the largest bank. Now I don't know if banks do this or not. But the point is very tight controls now are possible which was unthinkable just 25 years ago.

Finally, I insist that modern computer systems are difficult to subvert even by trusted employees because of their built-in security features. This is something that just has not been emphasized sufficiently.

It may be true that in early operating systems that were developed without any concern for security, a programmer could abuse it or any computer user could abuse it.

Modern systems really do have a lot of security features. I know myself in my daily work, security is a constant concern. We have a mythical character that we use. He is called the malicious programmer. I don't think a day goes by that we don't ask what could the malicious programmer do with this product that we are developing.

Another thing is that people seem to have the impression that computer systems are monolithic, that if I have a terminal connected to a computer, I can get at everything and I can do everything. That is not true. All I have is access to the records and files that I am allowed to have access to.

Now it would be very difficult for me to get at anybody else's files. I don't think that people understand the size and the scope. We are talking about monstrous filing cabinets. But you have to understand that a human being has to analyze those things before it makes any sense. If you have a machine go through records automatically retrieving information you are going to get absurdities.

A friend of mine was asking for direct access and operating systems. These are all computer terms. He got back an abstract with a report on swine feeding systems, because the key words were "direct access and operating systems."

It takes human intelligence to make any sense out of it and these filing systems are so vast that it is hard to go through it. It is very hard to find anything that you are looking for if you are not authorized to have it.

At my own computer installation, and I checked this, we have 1,200 disc packs. Now these are just the active disc packs. There are many others that are scratch packs. One pack holds many, many files. You would have to know specifically what the file was and where it was located, but there are access controls so that even if you could locate the pack that you were looking for you would be denied access to it because you are not on the authorization list.

In addition to 1,200 packs, we also have 13,000 tape reels.

Therefore, I could only subvert the records entrusted to me, but it is known that they are entrusted to me, and thus I am accountable.

I think that modern operating systems have really strengthened the security and have really increased the accountability.

It would be impossible for me to both defraud my company and to get away with it. Now this is the practical side. Theoretically, perhaps a programmer might be able to find a loophole in the system, but it would be extremely difficult for him to even practically exploit it.

I think that people who claim computer crime is easy don't really understand computer systems. Let me give you an illustration.

Rifkin, in the Security Pacific Bank theft did contemplate a computer crime, although the crime he committed in no way involved a computer.

He had attended a panel session on computer security with Parker of SRI, and was apparently smitten with Parker's notion of a "Trojan Horse" computer crime. But Rifkin was a programmer. He was not a computer crime theorist. He was faced with the reality presented by

Security Pacific Bank and he rejected computer crime for being too complex. I think that is a quote from Rifkin.

Instead, he impersonated a bank officer over the telephone to fraudulently transfer money. What he did was he contented himself with the more possible crime.

White collar crime I don't believe is going to disappear, but the machine should make it more difficult and its detection easier. Automated record keeping is not the environment in which crime can flourish.

Now I would like to turn to considering the adequacy of existing law. It has been argued that this bill is desirable because present law does not specifically cover crimes committed by computer. I believe that that is an equivocation.

Of course, present law doesn't cover theft by computer or by filing cabinet or by adding machine. It is clear to me, and I hope it is clear to everybody that if one steals money or goods by manipulating a computer or a filing cabinet, the offense under current law is larceny.

In the *Dog Track* case, nobody noticed our theories on the intangibility of computer data or effective difficulties of prosecuting computer crime. They were prosecuted for grand larceny. I believe that is exactly what they should have been.

I believe similar comments will apply to remaining crimes of fraud and embezzlement that this bill attempts to forbid.

What I think is true in that equivocation is that the Federal Government does not have the jurisdiction. This is not because of antiquated law, these 40 statutes of the Federal law which failed to foresee computers, but because local authority has jurisdiction. Such crimes are covered not by the United States Code, perhaps, but by State code.

I went through some of Susan Nickam's writings.

Mr. MARKMAN. Mr. Taber, I am sorry to interrupt. I am just wondering if we could perhaps draw your testimony to a conclusion.

Mr. TABER. Sure.

Mr. MARKMAN. I think there are a number of questions that everyone is going to have. The entire record will be placed in the record.

Mr. TABER. Very good.

Mr. MARKMAN. We are just running a little bit behind time. We want to apologize to you for that.

Mr. TABER. I think this bill is similar to mail fraud and wire fraud and telephone fraud statutes. I don't think that these are straightforward criminal laws but enabling acts. I think that they enable Federal law enforcement to intervene in a large number of common criminal matters.

What I question is: Do we really want Federal authorities to intervene in cases like this, and if so, can they do so effectively.

If you intend real computer crimes, I do not think there will be much to do. I think that this bill will be an unthumbed section of the United States Code.

But if you mean bookkeeping crimes, what I fear is that you will risk damaging the State's interest in prosecuting these crimes themselves and you will risk bogging down Federal law enforcement with too many common criminal cases.

I think that things like that have happened in the past.

The other thing is, what kind of bothers me is, so far as I can tell, the business community who is supposed to be suffering all this computer crime has not asked for this protection. So far as I can tell, they remain apathetic. It is supposed instead by a few prosecutors and is supported by a number of computer security specialists. I think that—well, going through the newspapers and the articles in *Computer World* and *Datamation*, the computer security outfits don't have a good reputation. Now that is not all of them. There are some outstanding exceptions. They have been criticized for being self-proclaimed experts and with little real knowledge of computer security.

They have been criticized for promoting unfounded scare stories and some of these scare stories were cited here in testimony. These were some of the fictitious cases I have mentioned and they promote these stories in order to sell insofar as I can tell, useless security gadgets.

One security specialist, Mr. Wasserman, of Computer Audit Systems has called his colleagues purveyors of snake oil.

A lot of the input to the Senate for this bill has been provided by computer security sources. I don't find that encouraging. I think it will be a pity if private interests foist unwitting commitments on us.

Mr. MARKMAN. Thank you very much, Mr. Taber. Your writings and your scholarly articles on this subject have been extremely helpful to the committee thus far. If you have no objections, we would like to put them in their entirety in the record on this.

Mr. TABER. Thank you.

[The material referred to above appears in the appendix.]

Mr. MARKMAN. I would also like to say to Professor Dertouzos that if there are any chapters of the book you have edited that you would like to include in the permanent record, we would be glad to do that as well.

I have just a couple of questions, Mr. Taber. One of the concerns of many of the Senators on the committee about this bill—and I think it has been alluded to earlier—is that there is significant disagreement as to what constitutes “computer crime” in the first place. At this point in the legislative process, we still have not resolved what seems to be a very basic and very threshold question. You touched further upon this in your written testimony, again, I know, but could you tell me what is your precise definition of a “computer crime”?

Does it make any difference whether or not a computer is an integral and indispensable element in criminal activity or whether it is simply used in the manner of a filing cabinet or some other more mundane facility?

How do we define a computer crime?

Mr. TABER. I do not believe that computer crime can be meaningfully defined. I think it is a buzz word. The newspapers may enjoy it. It is something of the same nature as the term “white collar crime.” I believe there are basic crimes, theft, so far and so on, but I think that “computer crimes” is a meaningless term.

Mr. MARKMAN. How expert, in your opinion, do law enforcement authorities have to be in the area of computer technology in order to effectively prosecute computer crimes? What recommendations, if any, would you have for developing this expertise?

Would you agree with Mr. MacFarlane, for example, that the expertise needed to detect and prosecute these crimes is not substantially greater than it would be for other crimes that law enforcement officials are more routinely involved in, such as antitrust matters?

Mr. TABER. As a matter of opinion, I would agree with him on that. As a matter of fact, to prosecute computer crime, the act of cooperation of the installation personnel, you are going to have to have it.

It would be very difficult for law enforcement to say burst in say gangbuster style and try to find the evidence of the crime. The amount of records that a large computer installation keeps is just massive. How do you find it? You just absolutely need their help and cooperation.

Mr. MARKMAN. I would just like to clarify. You are satisfied at this point that Senate bill 240 does protect computer programmers adequately with respect to essentially harmless instances of unauthorized use?

Mr. TABER. Yes, I do. By the way, if I may comment on that a little bit more. I would like it somehow understood, if it can be, that it is not the intent of this bill to stifle creativity. The original wording of unauthorized access I think may have had that effect. Now I can't pretend that it was a serious effect. It hasn't been that long. But since unauthorized access is taken out of the bill, I don't think the message has gotten out to other people that it is no longer an area of concern. There could still be some left over from the previous wording that would make programmers unduly cautious in experimenting with the computer.

Mr. MARKMAN. Thank you very much.

Mr. NASH. Mr. Taber, in the initial hearings on June 21, 1978, there was a quote that said, talking about computer crime, "it is a criminal activity that is difficult to detect." Is that true?

Mr. TABER. Well, I am not sure what it means. Again let us be specific. Supposing I altered some record in my custody. Now the fact that I was logged on to the machine and the fact that I was the only one who had the authority to access that, I think would identify me as the most likely person to have committed this offense.

Do you see what I mean?

Now it is true that the program that does it might disappear and might not be in the system, but I don't think that is significant.

Also, I haven't seen anybody mention that most computer installations have all sorts of backup procedures. We are very much aware that we could have a computer failure, the disc pack that I mentioned, God forbid, like a head crash which is our term for it, that wipes out the pack.

It is necessary to have periodic backups just in case you get a disaster like that, you can recover.

It seems to me that the idea of suddenly altering a record would be caught through all the backups. You would just be tracing back through backups that are taken every few days. I think there would be many traces of a crime that would be perhaps technically you could obliterate them, but practically, no.

Again, we keep getting into the practical versus the theoretical.

Mr. NASH. How about the next phrase, that computer crime is "very profitable."

Mr. TABER. Oh. Well, I disagree with people who say that it is very profitable. I think that the computer crime—

Mr. NASH. Could it become very profitable to you if you were so inclined?

Mr. TABER. I fail to see how. The records that I have are of no interest to anybody except my company. About the only practical crime that I can see a programmer such as myself committing is perhaps stealing a program and trying to peddle it. I think that is adequately covered by existing law, theft of trade secrets.

Mr. NASH. Then the last phrase was that computer crime is "easy to commit."

Mr. TABER. I do not believe these crimes are easy to commit. The programing is very complex and difficult. Most of my time is spent debugging my programs. I do not write perfect programs that work correctly the first time. It takes a lot of resources.

Programing, I would like to say, is kind of like a one-man effort. You do it alone with pencil and paper. But the testing part, the verification of the program has to be an organized, cooperative effort. It takes organization. That is exactly what is wrong with the "Trojan Horse" crime. There is no way to test it. It would have to work perfectly the first time. I just don't believe there is a programmer in the country who could do it. It is not just a few instructions, it is hundreds of instructions.

Mr. NASH. Why is it, do you suppose, that this mystique has built up?

Mr. TABER. There is widespread misunderstanding in the popular mind of what a computer is and what it does. I brought a little portable computer home from work. My son's friend was very disappointed because it didn't have flashing lights and you know, it was just a little desk top model. But he asked me to ask the computer what the weather is going to be. There is just nothing to say. Where do I begin to explain what a computer is and what it does? There is a very widespread misunderstanding. Computers are not intelligent. They do not think. They are not God.

The only creative part of the computer is the programmer who puts the program in it.

Mr. NASH. The audit potential of the various computers I guess depends on what that particular computer is being used for. Are computer auditors better able now to audit and track down fraud today than they were 10 years ago when you were programing?

Mr. TABER. I don't really understand quite what you are asking me. I think that the computer increases your ability to control your assets.

Mr. NASH. Let us say you were an unauthorized computer user, if an auditor said "Aha, Taber is obviously using this computer for other than business purposes," is the auditor's ability to find out if you are doing that increased today more so than it was 5 years ago?

Mr. TABER. I really don't know.

Mr. NASH. The last think is, other than the *Seidlitz* case where they did drop a count, do you know of any computer fraud case or computer abuse case that has been dropped for lack of an adequate statute to prosecute?

Mr. TABER. My understanding is there is not one case of computer crime that was thrown out of court; they have been convicted.

Now even in the *Seidlitz* case, Seidlitz was convicted and his conviction was upheld on appeal. It was just one charge that was dropped.

Mr. NASH. Just one charge that was dropped.

Mr. TABER. Yes.

Mr. NASH. Thank you.

Ms. ZEBROWSKI. Thank you, Mr. Taber.

I realize that many of your comments come from your personal experience as a programmer. I would like to take that one step further.

Do you see any impact on your day-to-day operations as a programmer from legislation such as we have before us?

Mr. TABER. Yes. As originally worded, with the unauthorized access, I do believe it has impacted me. I don't pretend it is a serious one, but I could see where it might be serious for others.

My own company very tightly controls what use is made of their machinery and they do so for security reasons. I believe that they became much tighter as a result of this bill originally being introduced. Now there is no way I can prove that, but that is what I suspect happened. Suddenly, our printouts all had that our machines were for internal use only, for official business use only.

Ms. ZEBROWSKI. Whereas before they were not?

Mr. TABER. They didn't say that. I assume it has always been company policy that the machines not be used except for business purposes. Nothing was said to me about it.

Ms. ZEBROWSKI. Many of your comments go to the current state of the art. Professor Dertouzos has testified that in the future we will be increasingly dependent on increasingly complex computers to do a variety of activities, involving our finances and our personal information and most everything else apparently in our day-to-day functioning.

Do you see that these increasingly complex computers will have an effect on the ability of individuals to detect and investigate crimes or abuses or misuses of those computers?

Mr. TABER. I simply don't know. The thing is that I would like to shy away from future predictions.

Ms. ZEBROWSKI. I have no further questions.

Mr. MARKMAN. Thank you very much, Mr. Taber. We very much appreciate your testimony. It has been extremely helpful.

Ms. TABER. Thank you.

[The prepared statement of Mr. Taber follows:]

PREPARED STATEMENT OF JOHN K. TABER

Mr. Chairman, members of the committee, my name is John K. Taber, I am a computer programmer, and I speak strictly as a private person. I do not represent any organization or other person.

The revisions made by this committee to the Federal Computer Systems Protection Act are very pleasing, and I am very grateful. The revisions corrected problems that I was very worried about. I believe that the bill could become law as now written without the potential of harm to the data processing community. Nevertheless, I am not enthusiastic. Although major problems are corrected, the bill remains unnecessary because:

First—computer crime is an insignificant problem and, second—existing criminal law is adequate.

The impression that computer crime is a serious growing problem is false, and is largely due to misinformation in the media. The Wall Street Journal in April 1968 carried the first ever computer crime story under the headline, "Whir, Blink—Jackpot! Crooked Operators Use Computers to Embezzle Money."

This tabloid headline does not inspire confidence in the accuracy of the article, which recounted three computer crimes. The crimes were real but two of them

occurred before the firms in question had computers, and the third case was indeed a genuine computer crime. In 1965 a programmer at the National City Bank of Minneapolis programmed the new checking system to ignore his overdrafts. Probably, he did not intend to steal—he meant to make good on his overdrafts, but he lost control and was \$1,357 overdrawn when caught. He received a suspended sentence and was forced to repay the bank.

The Wall Street Journal had only one case out of three right. As it happens, in computer crime stories, this is a high achievement of journalistic accuracy, scarcely matched by any other major paper.

The second genuine computer crime case is the Flagler Dog Track trifecta theft in Florida in 1977. It is also the sharpest example I have met with of a computer crime. A gang at the track colluded to skim money from the trifecta pool. In trifecta betting, one picks 1st, 2nd, and 3rd place dogs in a race. Winners, if any, are paid from a pool formed by the losers' money, at odds determined by the betting. Odds are not posted because the computation is lengthy, and even with a computer, the race may be over before the odds are computed. The Track used two PDP-8 computers, one as backup for the other, both of them computing odds and payoffs together. In the theft, the computer operator stopped one computer just before its program began the odds computation. Computers usually have an address stop mechanism by which the operator can specify the location of a program instruction in storage at which the computer halts execution. The operator, using the console switches, then "deducted" a number from the total of losers in computer storage and added the same number to the total of winners, also in storage. A confederate had posted the operator with the winning dogs. The operator then pressed the start switch and the program continued its computations, but now with altered totals. Later, the gang would print the additional winning tickets and cash them in. The computers also printed a report for track authorities but since there wasn't enough time to tamper with both computers, the gang submitted only the false report of the doctored computer, and did away with the incriminating report of the second computer.

The skimming was revealed by a tip to the authorities in late August. Martin Dardis, the investigator, was brought into the case in Sept, one day before the season was over, and cracked the case wide open in just three days. I think it was an outstanding job of police work. By the way, in the opinion of the authorities, the crime could never have succeeded without lax auditing and procedures on the part of the Track. Auditors were supposed to compare both computer reports, but failed to do so. There was also inadequate accounting of tickets, so that the forged tickets were not detected as they should have been. The amount stolen is probably unknown. Newspapers variously reported \$400,000, \$500,000, and \$1,000,000. But these are newspaper guesses, and I suspect that not even the thieves can state how much they actually stole.

I tend to stress this case because it is an excellent example of a genuine computer crime. By computer crime, I mean a crime in which a computer is directly and significantly an instrument of the crime. There are only two of which I am aware—the Minneapolis case, and this one.

It is reasonable to suppose that there must be a few more of which I am presently unaware, but certainly not hundreds. Also, in Parker's collection of cases, there are perhaps a dozen more anomalous cases that I would argue are not computer crimes, but which one could in all fairness argue that they were. But these two cases, in contrast, are not disputable. I judge that there are about a half dozen such cases, known and unknown. In short, genuine computer crimes are extremely rare. And when they do occur, they present no problems in the prosecution of the wrongdoers. Mr. Dardis' most serious problem was the time constraint imposed on him by the close of the season. The Minneapolis case was prosecuted in Federal court under existing U.S. law, and the Flagler case in state court under existing Florida law. No prosecutorial problems have been claimed for these cases.

To repeat, there are very few genuine computer crimes. But there are many crimes incorrectly called computer crimes. These crimes are various bookkeeping crimes that usually involve false inputs to an automated record keeping system to effect a fraud or theft. Some "computer crimes" cited in testimony here to support the bill are purely fictitious. They have never happened and originate in folklore. Other crimes, also cited in testimony here, really happened, but never involved a computer even in the remotest way. Still other crimes really happened in a computerized environment, nevertheless the computer played no instrumental

role. These bookkeeping crimes are the bulk of the real, nonfictitious, so-called computer crimes.

How many all told? The GAO found 69 such cases in the Federal Government, the largest single user of computers in the world. Parker, of SRI claims 633 cases of "computer abuse", which term is not to be confused with "computer crime". Roughly, a total of 700 cases, some unknown number of them criminal, over 30 years. In other words, if we grant the most exaggerated claims just for argument, computer crime however erroneously understood, has a completely insignificant incidence rate. Statistical error alone would swamp such a puny crime rate.

Parker, without justification, estimated an annual loss of \$300 million a year, a figure cited in testimony for this bill. That is the most exaggerated figure ever claimed for computer crime. But grant it just for argument. The U.S. Chamber of Commerce estimated an annual loss due to white collar crime of \$40 billion. Thus, computer crime losses, however exaggerated, is a drop in the bucket. It amounts to three-quarters of 1 percent of the white collar crime rate.

The GAO figured an average loss per case of \$44,000. Parker figured an average of \$450,000 per case, more than ten times the GAO figure. The only possible conclusion is that both the GAO and Parker cannot be right. The basis for Parker's figure has not been published. But the GAO's was. The GAO basis is good, and their figure is therefore more credible.

But what disturbs me most is that this bill originates in, and is justified by, contradictory and incomplete studies, with little validity if any. Because we do not have to grant these exaggerated claims. I have examined most of the extant computer crime studies. The best of the lot, at least for the veracity of its figures is the GAO study. There is an early private study sponsored by a Swedish insurance company, in 1970 which is laughable. I have a number of objections to SRI's studies, which will be published shortly. In brief, Parker's cases include abuse and non-abuse; crime and no crime; and computers and no computers. The study is inconsistent even in its own terminology, vacillating between abuse and crime in the most confusing manner. It rigorously defines terms then ignores its own definitions. The cases are mostly newspaper items, sometimes wildly inaccurate, provided by clipping services whose personnel can't tell a computer from a credit card. The study denounces newspapers for inaccuracies, but schizophrenically relies on them almost exclusively. Several of the cases are folklore, and could not have possibly occurred in fact. The cases are rarely documented, except for a news item, and sometimes not even that. The overwhelming majority of cases are unverified, in spite of the fact that SRI claims they are. What Parker means by verified is that he has assigned them a credibility weight based on his judgement of the completeness of a newspaper article. This is unacceptable by any scholarly standard except as the crudest sort of preliminary work.

Turning to the GAO study, the soberest of the lot, it too is far from perfect. It tries to make more of a case for computer crime than its own data support. It has the annoying habit of citing irrelevant cases not in its own data for their more impressive figures, borrowed on the whole from SRI. But from it, one can conclude that computer crime is an almost non-existent problem.

In short, the intellectual basis for this bill simply will not bear examination. Must we pass criminal law on such shaky grounds as that? Shouldn't the intellectual basis for a proposed law have some semblance of reality? And if a bill is unfounded, surely that is an end to it?

Now in contrast to these exaggerated claims, the American Bankers Association in 1978 conducted a survey of automatic teller machine operations. The ABA found that automated systems were safer than paper-based manual systems. Losses were either non-existent, or when they did occur, were less than in manual systems. In the few cases when loss did occur the average was twenty dollars.

Much earlier, in 1972, the bankers reported that in no case of bank fraud was the computer instrumental. This was in a report "A Study of Internal Frauds in Banks" by the Bank Administration Institute.

In other words, bankers have repeatedly claimed that they do not have a security problem with automated systems. Although I know of no other studies comparable to the banker's, I think the studies would show the same results for other businesses. The truth is that computer crime is not easy to commit, as you have been told in testimony here. On the contrary, computer crime is very difficult.

The fundamental fact of automated record keeping is that the books are removed from people and placed in the custody of a machine. The records, now magnetic blips, are not humanly detectable without the intermediary of machinery and an enormous amount of programming. Automation sharply curtails the number of people who can get at the books. In contrast, before computers, there was an office building full of clerks, any one of whom might have been tempted to juggle the books, and capable of doing so. The computer has tremendously increased the power of management to monitor and control their books and assets. Before computers, it would be unthinkable to routinely verify all accounts in even an ordinary sized bank. Auditing was based on sampling. But now, all accounts, even in the largest bank, can be verified routinely. Whether or not banks do, of course, I don't know, but the point is, very tight control is now possible that would have been unthinkable just 25 years ago.

Finally, modern computer systems are difficult to subvert even by trusted employees because of their built-in security features. Computer systems are not monolithic, as a layman might fancy. Their design enforces both accountability and division of responsibility. For example, I have direct, continuous access to a very large computer system that contains perhaps valuable records. But that doesn't mean that I can make the computer do anything I want. I have access only to the records that have been delegated to my care, and I cannot get at any others. For one thing I don't know where the other files are located—they are perhaps not in the computer or attached to the computer. They are swallowed up in one of 1,200 disk packs, which contain literally thousands and thousands of files, or in one of 13,000 tape reels. It would take me years, if not a lifetime to locate the file of interest. And even if I knew where that file was located, the operators would refuse to hook me up to the disk or tape containing it because I am not on their list of people authorized to use it. I can only subvert the records entrusted to me, but it is known that they are entrusted to me. Thus, I am accountable. It is impossible for me both to defraud my company and to get away with it.

Computer crime is not easy, and people who claim that it is don't understand computer systems. Frankly, I doubt that they even understand security. Rifkin, for example, in the Security Pacific Bank theft, did contemplate a computer crime, although the crime he committed in no way involved a computer. He had attended a panel session on computer security with Parker, and apparently was smitten with Parker's notion of a "trojan horse" computer crime. But Rifkin, unlike computer crime theorists, was a programmer, and faced with the reality presented by Security Pacific Bank, rejected computer crime for being too complex. Instead, he impersonated a bank officer over the telephone to fraudulently transfer money. He contented himself with a more possible crime.

White collar crime is not going to disappear. But the machine should make it more difficult and its detection easier. Automated record keeping is not the environment in which crime can flourish.

Now, let us consider the adequacy of existing law. It has been argued that this bill is desirable because present law does not specifically cover crimes committed by computer. That is an equivocation. Of course present law doesn't cover theft by computer, or for that matter by filing cabinet or adding machine! It is clear to me, and I hope that it is clear to everybody else, that if one steals money or goods by manipulating a computer or a filing cabinet, the offense under current law is larceny. In Miami, nobody noticed our theories on the intangibility of computer data, or the fictive difficulties of prosecuting computer crime. The Flagler Track thieves were prosecuted for grand larceny, exactly as they should have been. Similar comments apply to the remaining crimes of fraud and embezzlement that this bill attempts to forbid.

But what is true in that equivocation is that the Federal government does not have jurisdiction. Not because of antiquated law which failed to foresee computers, but because local authority has jurisdiction. Such crimes are covered, not by the U.S. Code perhaps, but by state code. Furthermore, state law covers not just the basic acts but various aspects of the acts in a very comprehensive manner. The section on theft, theft by misrepresentation, fraud, embezzlement, and their related aspects, is one of the fatter sections of the Annotated Penal Code of California.

In addition, the California Penal Code also proscribes the following acts:

1. Theft of trade secrets, 499c. This statute is directly applicable to theft of programs and data. There is no requirement to demonstrate asportation. I would

like to point out that in the *Ward* case in Calif., which involved just such a theft of a program, Ward was convicted of a dual charge of theft of trade secrets, and grand theft, CPC 484a. It appears that the courts in practice are pretty reasonable about interpreting tangibility and asportation.

2. Theft of services, 532. This statute directly covers theft of computer usage, that is, using data processing resources without the permission of the owner.

3. False record entry or alteration, 471. This statute directly covers falsification of records, whether or not maintained in an automated system.

4. Malicious mischief, 594. This statute is directly applicable to cases of destruction or tampering with computer data or programs, or the operation of a computer system. And malice, I understand, is determined by the facts of the case.

5. Criminal trespass, 602j. This statute covers interference with a computer system. The offense is a misdemeanor.

6. Forgery, 470. Applicability of this statute is not immediately apparent, but it may prove a powerful sanction. It covers the case of using an account or password not one's own to make use of a computer system. The account and password are considered legally to be "signatures," thus using a false one is forgery.

7. Burglary, 459. This statute is indirectly applicable. The commission of a felony on someone else's premises (for example, a computer installation) triggers burglary. The fact that a programmer is privileged to use the computer by the owner is no defense in Calif. (it is in some other states, however). Thus, the "authorized" programmer who steals a program may be charged with burglary as well as theft of trade secrets, or even simple theft.

In addition, other statutes may apply depending on the facts of the case and the legal requirements to support the charges. These are theft, Calif. Penal Code 484a; credit card abuse, Calif Penal Code 484d through i; and telephone abuse, Calif Penal Code 474.

I do not know the Codes of other states but I would be astonished if they were any less comprehensive than California's. It seems to me that these statutes provide complete protection for any thinkable "computer crime".

The Federal government itself also enjoys an array of existing law applicable to computer crime. Susan Nycum has listed about 40 statutes in a paper submitted to the Government Affairs Committee, which I won't repeat here, but I do recommend their being reviewed. I do not think that they have been antiquated by the computer as has been claimed. The Federal prosecutor's difficulty is jurisdiction, not antiquated law. In the *Seidlitz* case, which involved the theft of a program, the prosecutor charged Seidlitz with wire fraud. It is true that the court disallowed a second charge of interstate transportation of stolen property, but even here I think the difficulty of applying Federal law has been overstated. Perhaps the prosecutor really was in error. The fact is that Seidlitz was convicted of the basic charge of wire fraud. The mystery to me is why the Federal prosecutor assumed this case in the first place. Surely Maryland law is adequate to prosecute Seidlitz for his wrongdoing. It seems to me that the real offense was theft of trade secrets; in other words, a state offense. But even so, why wire fraud when the U.S. Code has an even more directly applicable statute that could have been applied with more justification? I refer to section 641, which forbids theft of public money, property, or records, and according to Mrs. Nycum "any misappropriation of software (in the custody of the government) is a violation of section 641." That is a pretty good description of the *Seidlitz* case, where a private firm's program rented to the government was stolen from a Federal Energy Administration computer. I think the prosecutor erred in a couple of ways, and it really isn't fair of him to blame the computer for his own errors.

To recapitulate. I have tried to show that "computer crime" is a rare and insignificant problem. So far, I have encountered only two cases that are definitely computer crimes, and I think that there are a few more. In contrast to SRI's study, there are other studies which indicate that losses are rare and laughably small.

I have also tried to show that existing law does cover these crimes, and covers them comprehensively. My purpose is to burn off the fog of misinformation that envelops "computer crime." I hope that I have succeeded so that the real issue can be seen and discussed.

The real issue, not to skirt it any longer, is Federal jurisdiction, or better, Congress' policy on Federal jurisdiction.

This bill is similar to the mail fraud and wire fraud and telephone fraud statutes. These are enabling acts, rather than straightforward criminal law, which

permit Federal law enforcement to intervene in a large number of common criminal matters. Such power to intervene, if it can be pegged to interstate commerce, is a settled issue. But does Congress want Federal authorities to intervene in this case, and can they do so effectively? If you intend real computer crime, Federal law enforcement will have little to do, and this bill will become an unthumbed section of the U.S. Code. If, on the other hand, you intend to go after bookkeeping crimes, you risk vitiating the states' interest and ability to prosecute these crimes, and you risk bogging down Federal law enforcement with too many common criminal cases. In testimony here, the FBI asked for 250 more people, and that is just for starters.

For computer crime, that is way too many, and for bookkeeping crimes, I suspect that won't be enough. Are we prepared for that kind of commitment, and most important, will the Government stick to it, if it's made? Past performance is not auspicious. Federal law enforcement is bored silly with car thefts and bank robberies, and suddenly today, after years of jailing joyriders and petty bank bandits, Federal law enforcement decides it has better things to do, and these thousands of cases can be handled by the states after all. However, over the years, the states lost their capacity, and worse, their interest, and are now faced with the painful burden of reallocating resources and gearing up to resume jurisdiction.

So far as I can tell, the business community, the supposed victim of all this "computer crime", has not asked for this protection. They certainly are not storming Congress, demanding this bill. They remain apathetic. It is supported instead by a few prosecutors, whom I suspect find "computer crime" a glamorous issue. It is also supported by a gaggle of commercial firms that specialize in "computer security", a product that apparently has not found its market yet. The commercial interest of these firms seems to me to be obvious. Phil Manuel, one of the authors of this bill is executive vice president of Guardsmark, Inc., a computer security outfit. August Bequai, whom I understand is another author of this bill, is, according to your staff, a lawyer for ASIS, an umbrella organization for security firms. Computer security outfits, with few exceptions, do not enjoy a good reputation. They have been criticized for being self-proclaimed experts, with little real knowledge of computer security. They have been criticized for promoting unfounded scare stories in order to sell useless security gadgets to foolish companies. Joseph J. Wasserman, himself a security specialist and president of Computer Audit Systems, Inc., has called his colleagues "purveyors of snake oil." Much of the input to the Senate for this bill has been provided by computer security sources. That is not encouraging. It will be a pity if the zeal of private interest foists unwitting commitments upon us.

Mr. MARKMAN. Our final witness today will be Mr. Lee Falke, who is a prosecuting attorney from Montgomery County, Ohio, wherein Dayton, Ohio, is situated.

Mr. Falke is also the chairman of the board of the National District Attorney Association, an organization which has been a frequent and always a useful witness before the Senate Judiciary Committee.

We would all like to thank you very much for coming today, Mr. Falke. We look forward to your comments on Senate bill 240.

**STATEMENT OF LEE FALKE, CHAIRMAN OF THE BOARD,
NATIONAL DISTRICT ATTORNEY ASSOCIATION**

Mr. FALKE. Thank you, Mr. Chairman.

On behalf of the National District Attorneys Association, and I have to limit that on behalf really of the executive committee of the National District Attorneys, I am here to speak in opposition to the bill.

I would like to say for background that the National District Attorneys Association is an organization of over 7,000 prosecuting attorneys throughout the United States. We feel we are more or less in the front line, you might say, of the battle, the battle of crime.

To put things in perspective, I guess I would further like to say that we probably handle and have more prosecuting attorneys, probably

handle more criminal cases than any one of our major states, than the Federal Government does throughout the whole country.

So, we feel that we are quite expert in the matter of trying criminal cases and indeed, may be even more expert than the Federal district attorneys are.

I would like to say just a brief remark about the previous statements. I guess I basically agree with all of the three previous speakers.

I guess in answer to some of your questions about will this bill help us detect computer crime, my answer to that question is that I do not think that it does help detect computer crime.

There are many situations that we find ourselves in where evidence is very hard to come by. Many murders are a situation where there are only two people present; one is dead and the defendant won't talk. So, that is a very difficult type of crime to detect also. I don't think a special law would solve the problem, unless you could do something about the fifth amendment. That might help.

Before I came here just a day or two ago, a former Senator, Sam Ervin, was the speaker before a local bar association. He made a statement that I think the National District Attorney Association basically agrees with, and that is, the Federal Government has an insatiable thirst for power. The only thing to prevent it is for people to be eternally vigilant and that is why we are here.

We feel that Senate bill 240 basically projects itself too much into local government matters. Although I have to confess for the record that I am not particularly informed on the particular Federal statutes that the Justice Department has referred to in their previous testimony, I suspect that their limitation is not because they need a Federal computer crime bill, it is because of the limitation of the extent to which they have been authorized to go into local government, local crime problems rather than the national crime problems.

Mr. Don Parker has been referred to earlier. In his book, "Crime by Computer," he estimates that in 1980 we have 500,000 businesses with computers.

He further estimates that some place between 3 and 7 percent of the work force in the United States deals somehow with computer hardware.

I have no way of verifying that, but it appears to me that the interstate commerce clause of the Senate bill 240 would certainly authorize the Federal investigative agencies to go into every community in the United States as a result of that particular aspect of the bill.

I think that particular aspect the national district attorneys is particularly opposed to, the interstate commerce aspect of the legislation.

As to the governmental coverage of the legislation, the banking coverage, and the securities coverage, I would like to refer to the Stanford Research Institute International, a summary they made as of the end of 1978. Their estimate is and as has also been previously testified to that there have been 632 cases involving computer abuse in the United States since 1968. They estimate that of those 632 cases, 120 cases have involved the banking industry, or 18.9 percent. And Federal and local government, for 16 percent, and that there were 10 cases involving securities transactions, which is less than 1 percent.

Totaling those percentages, if the legislation would stand as to those three industries, as far as the past record is concerned, the legis-

lation would cover approximately 35 percent of the crimes that have been committed in regard to computer abuse.

On behalf of the national district attorneys, we would recommend that the legislation at least not be extended beyond those three types of industries.

From a practical standpoint, if we are not adding a whole lot of cases as far as investigation is concerned, because in 1977, the Stanford Research Institute also reports that they feel there was a total of 85 computer abuse cases in the United States in 1977, and 31 computer abuse cases in 1978.

They have a breakdown between vandalism, information or property theft, financial fraud or theft, unauthorized use or sale or services in those categories.

So, I could give you more details on that. I think they actually only show the financial fraud or theft part of the computer abuse cases as being 44 in 1977, and 12 in 1978.

I would like to suggest a positive solution to some of this. I think there are two positive solutions to the computer crime problem, if there is indeed such a problem.

I first of all believe that most State laws are broad enough to cover the types of theft that would be involved or the damage to the computers or the theft of the information. I think that computer hardware and programing is already defined as property in most of the States so that the laws that are presently in existence cover the problem from a State standpoint.

I frankly would have to disagree with the Attorney General McFarlane. I do, however, believe there is some need for some specialized knowledge, some assistance in that area.

I would like to recommend, frankly, that that assistance be supplied through the Federal crime lab, that their area of responsibility or assistance be broadened so that they would develop some experts in this field, as well as many other fields. We need experts sometimes in auditing problems and things of this nature.

So, I think that is something that they could provide that would be very helpful for local prosecutors, but I feel that when the case has been investigated and when we have the expert help that the local prosecutors are quite ready, willing and able to try crimes of this nature.

Another area where I think we could use some assistance and that is the Justice Department or perhaps it could be done through the Federal crime lab on occasions, we need records from other States. Their assistance in those areas would be helpful, but it is not the type of situation or a problem that exists only in regard to computers, it is the problem that exists in regard to all types of investigation. It could be homicide. It could be a theft. It could be any other types of crime.

So, it needs to have broader coverage than just computer problems.

I do not know if the Senators are aware, there is presently what is called an executive working committee that has been established between the national district attorneys, the Justice Department, and the States attorneys general. We are working on some of those cooperative problems and sharing of information and investigation. So it may be that we will be able to solve some of those problems within

our own committees, but an ever-mindful eye from the Senators would certainly be helpful in that regard.

There is one aspect of this S. 240 that I particularly would like to comment on and that is the penalties section. I think the 200 percent penalty is a very intriguing idea. We certainly do not want to have criminals who benefit from their crime. I think perhaps new legislation is necessary in that regard, but not only for computer crimes but other types of thefts as well.

There are really no laws that would enable a judge to fine a defendant say \$1 million or something like that in the event he has taken that much money.

A further problem is that in most situations it is impossible to order restitution and send a person to jail at the same time. Restitution is usually only an element of probation. So, if a person is going to be sentenced to jail, he may have a nominal fine, but certainly there is no fine that I know of on the records any place that would allow someone to be fined a substantial sum of money.

So, I like that idea. I do however submit that it has some built in problems the way it is presently drafted and that is, that if the defendant is fined twice the amount he has taken, whatever money he has salvaged from his theft will probably be taken in the way of a fine and the victim would be remedyless as far as recovering his loss.

I would like to recommend that that sort of fine is a good idea, but some credit at least should be given for any amount that the defendant pays back to the victim. Maybe to encourage that we could give him a credit of say one and a half times that amount he pays back so that ultimately he would get a credit for some of the fine, but maybe not all of the fine.

There are some technical problems with the bill as we see it if it is going to be passed. As I say, we certainly recommend that it not be passed in its present form.

We note that the legislation itself limits itself to the use of a computer. It does not really direct itself to stealing the equipment or the hardware or the program and things of that nature unless the computer is used as a part of that theft.

Also, it only provides for a \$50,000 penalty in the event there is damage to the computer. Many computers, if not all of them have a greater value than that. I think the damage penalty ought to be the same as the penalty for theft.

I feel there is an attempt to exclude the types of computers that would be used for personal or family or household purposes, but it seems to me the way the exclusion clause is written that there isn't any type of case that would fit under the exclusion clause because it says that it excludes any computer designed and manufactured for and which is used exclusively for routine personal, family, or household purpose.

Well, by the time you go through all that, there would not be hardly any type of computer that would meet that definition.

I like the subparagraph (d), which talked about in the event there is Federal jurisdiction, the reporting, and the communication and things of that nature, I thought were good additions to the legislation if it is going to be passed.

In conclusion, I would like to say that on behalf of the National District Attorneys we oppose the legislation as being an intrusion into local government matters. We do not think it is necessary in view of the declination policy of the Justice Department. We feel they have already indicated they have too much work and can't handle the crimes that are assigned to them now.

We feel that there are some things that could be done in a positive way. We feel that some broadening of the services of the FBI Crime Lab would be beneficial.

We feel that the penalty paragraph has some real merit, if redesigned and applied to all types of thefts. But the particular form of the legislation we have to oppose.

Mr. MARKMAN. Thank you very much, Mr. Falke. I think we all appreciate your analysis of S. 240. I would like to say, incidentally, that you have really done double duty here today by anticipating some of the provisions that are in the proposed Criminal Code reform, among those being provisions dealing with restitution and the borrowing of other civil remedies for the criminal law. We appreciate your observations on that as well.

I have a couple of questions here. You indicate some concern about the fact that S. 240 will impinge upon areas that are presently within the jurisdiction or responsibility of the local governments. Hasn't this precedent, however, already been established. We have Federal wire fraud statutes and Federal mail fraud statutes which, if the Government interprets them as fully as they might, will probably do exactly the same thing.

Haven't we been successful in relying upon prosecutorial discretion in the past to insure that these are enforced in a responsible manner?

Mr. FALKE. I would say that in most situations, although it has been abused on occasion, and depending upon the direction of the Justice Department, it could easily be abused in the future.

I would say that frankly, the National District Attorneys have maybe slept on some of their responsibility in this area in the past. We have not been active in testifying, except for the last couple of years. But we do not intend to sleep on our responsibilities in this area in the future.

Mr. MARKMAN. Would you agree with Mr. Taber that "computer crime" is a pretty difficult thing to define in the first place? How would you define "computer crime"?

Mr. FALKE. I think I agree with Mr. Taber's analysis of that. I just think that what we are really talking about is a theft and what we are talking about is how you do it. I don't think we need the special legislation for it.

Mr. MARKMAN. I see. I want to thank you. Senator Laxalt's office has a few questions now.

Mr. NASH. First I want to get your support. Senator Laxalt introduced a bill abolishing the exclusionary rule giving the defendant a Federal cause of action under the Federal Tort Claims Act for any violations of his fourth amendment rights.

But, I want to say that on giving the fine to the victim, would that give the victim a vested interest in insuring a successful prosecution. Do you see any problems with that during the course of a trial?

Mr. FALKE. Are you saying he would be accused of altering his testimony in order to benefit from the prosecution?

Mr. NASH. If they had a substantial reward if there were a successful prosecution.

Mr. FALKE. I think that allegation could be made now. Most of the victims are, if there is any chance of recovering any money, they have already filed civil suit or they will be hoping to gain some recovery through the criminal action by way of the restitution or something that would be ordered by the court.

So, I don't think that would really change.

Mr. NASH. There is one other thing. You mentioned that the Stanford Research Institute said there were 89 computer crimes last year. Probably none of them happened in Dayton, but are there any evidentiary problems with this type of crime under the "business record" rule and putting records like that into evidence?

Mr. FALKE. We probably had one computer crime that happened that wasn't reported as a computer crime, or at least it kind of fits the broad definition of computer crime. We had a clerk in a credit office altering records, showing that people had assets that didn't actually have the assets. The defendants then who were conspiring with them would go and purchase automobiles and things like that. The credit records would show that they had sufficient wherewithal to pay back the money. So, they were sold goods. We successfully prosecuted that. We didn't have any problem.

Mr. NASH. So, you have never had to not prosecute a case because you did not have the statutory authority?

Mr. FALKE. No; I am not aware of any in Ohio, at all. I just don't think it is a problem.

Mr. NASH. Thank you very much.

Ms. ZEBROWSKI. Thank you for your testimony.

In a letter submitted for the record in 1978, a representative of the National District Attorneys Association, Mr. Kossack, indicated that the bill should be construed to include use of the computer as a coverup

Does the NDAA still hold that view and if so, could you elaborate?

Mr. FALKE. I am not sure exactly why Mr. Kossack testified that way. I am not sure what his reasoning was.

Ms. ZEBROWSKI. I only have one further question and then, if possible, I would like to submit some questions in writing for you to answer at your leisure.

Mr. FALKE. I would be glad to.

Ms. ZEBROWSKI. You indicated that you had a number of computer crime type prosecutions in your State. Could you describe them very briefly, what sort of cases that you are talking about?

Mr. FALKE. The only one that I know of is the one that our office handled and I already described that. That was the credit information fraud.

Ms. ZEBROWSKI. Are you aware of any States who handled computer-related offenses of an interstate nature?

Mr. FALKE. Well, I know that some—you know, I am sure that all of the major crimes involving the major amounts of money have involved some interstate transactions. Again, according to the Stanford Research Institute, there have been eight cases, at least as of January

1979, that are known to have involved more than \$10 million. I am sure all those cases involve some aspects of interstate traffic. I do not know of any of that causing any major problem.

Ms. ZEBROWSKI. In earlier testimony for this committee the Federal prosecutor involved in a local case, the *Seidlitz* case, indicated that it was a Federal prosecution for a number of reasons, including that local prosecutors found that they needed extensive cooperation with neighboring States. It was a particular problem because it was an offense involving Virginia, Maryland, and, in part, the District of Columbia. The local prosecutors felt they had some difficulty in gaining cooperating services from those other areas. Do you see that as a problem elsewhere?

Mr. FALKE. Yes, I see it in all types of crime. We right now have a major investigation going in regard to a national political figure. We have tried to get information from the Federal Government and they absolutely won't give it to us.

So, it is not only involving computer crime, it is involving any type of crime.

Ms. ZEBROWSKI. What about information from other States?

Mr. FALKE. Well, information from other States is one of the areas where I indicated that maybe the FBI crime lab—their services could be broadened so that they could assist us in getting some of that information.

Right now, it would depend upon the good graces of the prosecutor and police chief in some other jurisdiction as to whether he would help you get that or not.

Ms. ZEBROWSKI. Thank you very much. I may submit later questions in writing.

Mr. FALKE. Thank you.

Mr. MARKMAN. Thank you very much, Mr. Falke. We appreciate you coming and we appreciate the National District Attorneys Association's comments on this bill.

Once again, we would like to thank all the witnesses. We would also like to say once again that we regret the conflicts that the Senators on this committee have had today. We would like to say in behalf of Senator Hatch and Senator Laxalt and Senator Biden and the rest of the committee that this has proven to be a very informative day of testimony. It will undoubtedly be extremely influential in helping the committee make up its decision on Senate bill 240.

The committee stands adjourned, subject to the call of the Chair.

[Whereupon, at 1:10 p.m., the committee adjourned, subject to the call of the Chair.]

APPENDIX

96TH CONGRESS
1ST SESSION

S. 240

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

 IN THE SENATE OF THE UNITED STATES

JANUARY 25 (legislative day, JANUARY 15), 1979

Mr. RIBICOFF (for himself, Mr. PERCY, Mr. KENNEDY, Mr. INOUE, Mr. JACKSON, Mr. MATSUNAGA, Mr. MOYNIHAN, Mr. WILLIAMS, Mr. ZORINSKY, Mr. DOMENICI, Mr. STEVENS, Mr. CHILES, and Mr. NUNN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

 A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

- 1 *Be it enacted by the Senate and House of Representa-*
- 2 *tives of the United States of America in Congress assembled,*
- 3 That this Act may be cited as the "Federal Computer Sys-
- 4 tems Protection Act of 1979".

1 SEC. 2. The Congress finds that—

2 (1) computer-related crime is a growing problem
3 in the Government and in the private sector;

4 (2) such crime occurs at great cost to the public
5 since losses for each incident of computer crime tend to
6 be far greater than the losses associated with each in-
7 cident of other white collar crime;

8 (3) the opportunities for computer-related crimes
9 in Federal programs, in financial institutions, and in
10 other entities which operate in interstate commerce
11 through the introduction of fraudulent records into a
12 computer system, unauthorized use of computer facili-
13 ties, alteration or destruction of computerized informa-
14 tion files, and stealing of financial instruments, data, or
15 other assets, are great;

16 (4) computer-related crime directed at institutions
17 operating in interstate commerce has a direct effect on
18 interstate commerce; and

19 (5) the prosecution of persons engaged in
20 computer-related crime is difficult under current Fed-
21 eral criminal statutes.

22 SEC. 3. (a) Chapter 47 of title 18, United States Code,
23 is amended by adding at the end thereof the following new
24 section:

1 "§1028. Computer fraud and abuse

2 “(a) Whoever knowingly and willfully, directly or indi-
3 rectly accesses, causes to be accessed or attempts to access
4 any computer, computer system, computer network, or any
5 part thereof which, in whole or in part, operates in interstate
6 commerce or is owned by, under contract to, or in conjunc-
7 tion with, any financial institution, the United States Govern-
8 ment or any branch, department, or agency thereof, or any
9 entity operating in or affecting interstate commerce, for the
10 purpose of—

11 “(1) devising or executing any scheme or artifice
12 to defraud, or

13 “(2) obtaining money, property, or services, for
14 themselves or another, by means of false or fraudulent
15 pretenses, representations or promises, shall be fined a
16 sum not more than two and one-half times the amount
17 of the fraud or theft, or imprisoned not more than fif-
18 teen years, or both.

19 “(b) Whoever intentionally and without authorization,
20 directly or indirectly accesses, alters, damages, destroys, or
21 attempts to damage or destroy any computer, computer
22 system, or computer network described in subsection (a), or
23 any computer software, program or data contained in such
24 computer, computer system or computer network, shall be

1 fined not more than \$50,000 or imprisoned not more than
2 fifteen years, or both.

3 “(c) For purposes of this section, the term—

4 “(1) ‘access’ means to approach, instruct, commu-
5 nicate with, store data in, retrieve data from, or other-
6 wise make use of any resources of, a computer, com-
7 puter system, or computer network;

8 “(2) ‘computer’ means an electronic device which
9 performs logical, arithmetic, and memory functions by
10 the manipulations of electronic or magnetic impulses,
11 and includes all input, output, processing, storage, soft-
12 ware, or communication facilities which are connected
13 or related to such a device in a system or network;

14 “(3) ‘computer system’ means a set of related,
15 connected or unconnected, computer equipment, de-
16 vices, and software;

17 “(4) ‘computer network’ means the interconnec-
18 tion of communication systems with a computer
19 through remote terminals, or a complex consisting of
20 two or more interconnected computers;

21 “(5) ‘property’ includes, but is not limited to, fi-
22 nancial instruments, information, including electroni-
23 cally processed or produced data, and computer
24 software and programs in either machine or human

1 readable form, and any other tangible or intangible
2 item of value;

3 “(6) ‘services’ includes, but is not limited to, com-
4 puter time, data processing, and storage functions;

5 “(7) ‘financial instrument’ means any check, draft,
6 money order, certificate of deposit, letter of credit, bill
7 of exchange, credit card, or marketable security, or
8 any electronic data processing representation thereof;

9 “(8) ‘computer program’ means an instruction or
10 statement or a series of instructions or statements, in a
11 form acceptable to a computer, which permits the func-
12 tioning of a computer system in a manner designed to
13 provide appropriate products from such computer
14 system;

15 “(9) ‘computer software’ means a set of computer
16 programs, procedures, and associated documentation
17 concerned with the operation of a computer system;

18 “(10) ‘financial institution’ means—

19 “(A) a bank with deposits insured by the
20 Federal Deposit Insurance Corporation;

21 “(B) a member of the Federal Reserve in-
22 cluding any Federal Reserve bank;

23 “(C) an institution with accounts insured by
24 the Federal Savings and Loan Insurance
25 Corporation;

1 “(D) a credit union with accounts insured by
2 the National Credit Union Administration;

3 “(E) a member of the Federal home loan
4 bank systems and any home loan bank;

5 “(F) a member or business insured by the
6 Securities Investor Protection Corporation; and

7 “(G) a broker-dealer registered with the Se-
8 curities and Exchange Commission pursuant to
9 section 15 of the Securities and Exchange Act of
10 1934.”.

11 (c) The table of sections of chapter 47 of title 18, United
12 States Code, is amended by adding at the end thereof the
13 following:

“1028. Computer fraud and abuse.”.

"ADDITIONAL SUBMISSIONS OF J. D. MacFARLANE"

ARTICLE 5.5

Computer Crime

Editor's note: Section 12 of chapter 168, Session Laws of Colorado 1979, provides that the act enacting this article is effective July 1, 1979, and applies to offenses alleged to have been committed on or after said date.

18-5.5-101. Definitions.

18-5.5-102. Computer crime.

18-5.5-101. Definitions. As used in this article, unless the context otherwise requires:

(1) To "use" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

Source: Added, L. 79, p. 728, § 7.

18-5.5-102. Computer crime. (1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of: Devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than two hundred dollars, computer crime is a class 2 misdemeanor; if two hundred dollars or more but less than ten thousand dollars, computer crime is a class 4 felony; if ten thousand dollars or more, computer crime is a class 3 felony.

Source: Added, L. 79, p. 728, § 7.

ARTICLE 6

Offenses Involving the Family Relation

PART 4

18-6-403. Sexual exploitation of children.

WRONGS TO CHILDREN

18-6-401. Child abuse.

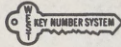
PART 1

ABORTION

18-6-101. Definitions.

The ruling granting the defendant's motion to suppress is reversed.

CARRIGAN, J., does not participate.



The PEOPLE of the State of Colorado,
Plaintiff-Appellant,

v.

HOME INSURANCE COMPANY and
Home Indemnity Company,
Defendants-Appellees.

No. 27984.

Supreme Court of Colorado,
En Banc.

March 19, 1979.

Insurance companies were charged with theft arising out of surreptitious procurement by their agents of confidential medical information concerning two hospitalized claimants. The District Court, City and County of Denver, George M. McNamara, J., dismissed the charges and the People appealed. The Supreme Court, Lee, J., held that procurement by telephone of confidential medical information concerning hospitalized claimants did not constitute theft of "thing of value" within meaning of theft statutes.

Affirmed.

1. Larceny ◀=6

Insurance company agents' surreptitious procurement by telephone of confidential medical information concerning hospitalized claimants did not constitute theft of "thing of value" within meaning of theft statutes. C.R.S. 78, 18-1-901(3)(r), 18-4-401(1)(a).

See publication Words and Phrases for other judicial constructions and definitions.

2. Statutes ◀=241(1)

Criminal statutes must be strictly construed in favor of defendant and they cannot be extended either by implication or construction.

3. Criminal Law ◀=562

Proof of moral turpitude is not alone sufficient to authorize a criminal conviction.

Dale Tooley, Dist. Atty., Brooke Wunnicke, Chief App. Deputy Dist. Atty., Denver, for plaintiff-appellant.

Holm & Dill, Professional Corp., Jon L. Holm, Denver, for defendants-appellees.

LEE, Justice.

The People appeal from the dismissal of theft and theft-related charges by the trial court at the close of the prosecution's case. The charges arose from the surreptitious procurement by agents of the insurance company defendants of confidential medical information concerning two patients of a Denver hospital. The trial court granted the dismissal because the medical information obtained was not a "thing of value" as defined in the pertinent statute and therefore was not subject to theft. We affirm.

The defendants hired an injury claims investigative service to obtain medical information reports on two claimants. Through the use of the telephone, an investigator for the service obtained a verbatim reading of the medical reports which he later transcribed and sent to the defendants. The actual medical records themselves never left the hospital file room; rather, only the medical information contained in the records was thus acquired.

The theft statute, section 18-4-401(1)(a), C.R.S.1973 (1978 Repl. Vol. 8), reads in pertinent part:

"A person commits theft when he knowingly obtains or exercises control over anything of value of another without authorization, or by threat or deception, and:

"(a) Intends to deprive the other person permanently of the use or benefit of the thing of value * * *."

Crucial to our determination of this case is the definition of "thing of value" contained in section 18-1-901(3)(r), C.R.S.1973 (1978 Repl. Vol. 8):

"Thing of value" includes real property, tangible and intangible personal property, contract rights, choses in action, services, and any rights or use or enjoyment connected therewith."

[1] The People argue that the confidentiality inherent in one's personal medical information is a "thing of value" within the meaning of the theft statute inasmuch as the confidentiality is intangible personal property. We do not agree with this expansive interpretation of the theft statute.

[2] In determining the meaning of criminal statutes, we are guided by the principle that such statutes must be strictly construed in favor of the accused and they cannot be extended either by implication or construction. *People v. Cornelison*, 192 Colo. 337, 559 P.2d 1102 (1977); *Cokley v. People*, 168 Colo. 280, 450 P.2d 1013 (1969); *Calkins v. Albi*, 163 Colo. 370, 431 P.2d 17 (1967).

As far as we have been able to determine, and no cases have been cited by the People to the contrary, confidentiality has never been considered as intangible personal property. Rather, the term intangible personal property has been held to be property which is merely representative of value, such as certificates of stock, bonds, promissory notes, patents, copyrights, tradebrands and franchises. *Black's Law Dictionary*, (rev. 4th ed. 1968). We, therefore, would have to expand unduly the traditional concept of intangible property if we were to accept the People's contention.

Furthermore, the General Assembly has specifically addressed the violation of analogous privacy interests in the criminal code.

1. Although traditionally there has been a civil remedy for appropriation of trade secrets, see *Trade Secret Litigation: Injunctions and Other Equitable Remedies*, 48 U.Colo.L.Rev. 189

Thus, it has authorized criminal sanctions for the theft of trade secrets, section 18-4-408, C.R.S.1973 (1978 Repl. Vol. 8),¹ unauthorized wiretapping of telephone or telegraph communication, section 18-9-303, C.R.S.1973 (1978 Repl. Vol. 8); eavesdropping, section 18-9-304, C.R.S.1973 (1978 Repl. Vol. 8); and unauthorized reading, learning or disclosure of telephone, telegraph or mail messages, section 18-9-306, C.R.S.1973 (1978 Repl. Vol. 8). The foregoing amply demonstrates that the General Assembly has the legislative competence, if inclined to do so, to make illegal the invasion of privacy or confidentiality. The legislature, however, has not chosen to apply criminal sanctions to the invasion of the confidentiality of medical information. We will not now do so by an unwarranted interpretation of the meaning of intangible personal property as it is used in the statutory definition of "thing of value."

In the civil context the legislature has considered the importance of confidentiality of medical information. Section 25-1-802, C.R.S.1973 (1978 Supp.) concerns confidentiality of patient records in the custody of health care facilities. Section 27-10-120, C.R.S.1973, provides that all information obtained in the course of providing services to the mentally ill in state institutions shall be confidential and privileged. Section 25-1-312, C.R.S.1973, makes records of alcoholics compiled at treatment facilities confidential and privileged. Section 24-72-204(3), C.R.S.1973, provides that public records containing medical and psychological data shall not be available for public inspection except in certain prescribed circumstances. The legislature, therefore, has taken specific steps to protect the confidentiality of medical information by creating statutory duties, the breach of which could serve as the basis for a civil remedy. However, the legislature has not imposed criminal penalties for violations of the confidentiality or privilege.

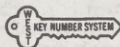
(1977), the legislature considered the increasing encroachment on this type of confidentiality as warranting criminal penalties.

[3] Finally, the acceptance of the People's contention that invasion of the confidentiality of one's medical records constitutes theft would have far-reaching ramifications. Conceivably, a person who committed one of the four recognized torts for the invasion of privacy² could be tried for theft. Also, the breach of one of the recognized privileges (e. g., husband-wife, attorney-client, clergyman-penitent, doctor-patient, accountant-client and psychologist-client, see section 13-90-107, C.R.S.1973) might possibly be construed as theft. In our view, such an expansion of criminal liability could not have been intended by the legislature when it adopted the theft statute. Although we agree with the trial court that the defendants' conduct was "reprehensible and outrageous," that conduct simply was not made criminal under the theft statute. Proof of moral turpitude is not alone sufficient to authorize a criminal conviction. *Shimmel v. People*, 108 Colo. 592, 121 P.2d 491 (1942).

Because of our disposition, it is unnecessary to address the issue of how to calculate the monetary worth of the medical information or the issue of whether the evidence established the element of permanent deprivation.

The judgment is affirmed.

CARRIGAN, J., does not participate.



2. According to *W. Prosser, Torts* § 117 (4th ed. 1971), the common law tort of invasion of privacy contains four distinct kinds of invasion of four different interests: (1) intrusion upon

PEOPLE of the State of Colorado,
Petitioner,

v.

Bruce FERRELL, Jr., Respondent.

No. C-1583.

Supreme Court of Colorado,
En Banc.

March 19, 1979.

People appealed from an order of the District Court, Mesa County, James J. Carter, J., which reversed defendant's county court conviction for obtaining goods of value by deception. The Supreme Court, Groves, J., held that there was no evidence that defendant's alleged deception in giving false name and address in credit application was relied upon by store's personnel so as to support conviction.

Affirmed.

False Pretenses ⇐ 49(5)

In prosecution for obtaining goods of value by deception, there was no evidence that defendant's alleged deception in giving false name and address in credit application was relied upon by store's personnel so as to support conviction. C.R.S. '73, 18-4-401.

Terrance Farina, Dist. Atty., James R. Alvililar, Deputy Dist. Atty., Grand Junction, for petitioner.

Dufford, Waldeck & Williams, Laird T. Milburn, Ware B. Flora, Grand Junction, for respondent.

GROVES, Justice.

The People appeal from the district court's reversal on appeal of the defendant's conviction in the county court. The county court had found him guilty of obtaining goods of value by deception in viola-

physical solitude; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation of name or likeness.

An Act

HOUSE BILL NO. 1110. BY REPRESENTATIVES Dodge, DeFilippo, DeHerrera, DeNier, Durham, Erickson, Kopel, Lillpop, Taylor, Theos, and Younglund; also SENATORS Cole, Meiklejohn, Woodard, and Zakhem.

CONCERNING THE "COLORADO CRIMINAL CODE", AND MAKING MISCELLANEOUS AMENDMENTS THERETO.

Be it enacted by the General Assembly of the State of Colorado:

ARTICLE 5.5

Computer Crime

18-5.5-101. Definitions. As used in this article, unless the context otherwise requires:

- (1) To "use" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
- (2) "Computer" means an electronic device which performs

logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

18-5.5-102. Computer crime. (1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of: Devising or executing any scheme or artifice to defraud, obtaining money, property, or services by means of false or fraudulent pretences, representations, or promises, or committing theft, commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than two hundred dollars, computer crime is a class 2 misdemeanor; if two hundred dollars or more but less than ten thousand dollars, computer crime is a class 4 felony; if ten thousand dollars or more, computer crime is a class 3 felony.

Robert F. Burford
SPEAKER OF THE HOUSE
OF REPRESENTATIVES

Fred E. Anderson
PRESIDENT OF
THE SENATE

Lorraine F. Lombardi
CHIEF CLERK OF THE HOUSE
OF REPRESENTATIVES

Marjorie L. Rutenbeck
SECRETARY OF
THE SENATE

APPROVED _____

Richard D. Lamm
GOVERNOR OF THE STATE OF COLORADO

ADDITIONAL SUBMISSIONS OF JOHN K. TABER

Kathy Zebrowski
Senate Subcommittee on Criminal
Laws and Procedures
6A Russell Senate Office Bldg
Washington, D. C. 20510

John K. Taber
609 Meadow Ave.
Santa Clara, Calif. 95051

Jan 11, 1980

Dear Kathy:

Attached is my article on the revised version of S240. The article is not an enthusiastic endorsement of the bill, but it does acknowledge the improvements, and speaking personally, I am very pleased and grateful for the revisions.

Whether or not the bill is a wise measure is hard for me to say. I'm quite sure that computer crime is an insignificant problem that does not merit special law. Logically and factually I think the bill is unnecessary, and certainly premature. But whether or not the bill is desirable anyway, I just can't say.

I have a few minor wording suggestions.

1. The bill's preamble, section 2 paragraph 2, reads

"losses ... of computer crime tend to be far greater."

There is no good evidence for this statement. According to the FBI, the average bank fraud is \$19,000 while according to the GAO the average computer crime is \$44,000. This is not "far greater", and the word far should be stricken. The bill will lose nothing by omitting far and will gain more accuracy. I am aware of SRI's figures, but they are not good evidence. By the way, in this connection, the Committee may be interested to know that the American Bankers Association surveyed Automatic Teller Machine security in 1978. The ABA found that ATM is far safer than paper based manual systems. Losses were few and averaged about \$20. Even saying that computer crime losses are "greater" than

other, comparable crime losses seems risky to me, and may eventually prove to be an embarrassment.

2. The preamble, section 2, paragraph 3, reads

"... opportunities for computer-related crimes ... are great"

"Are great" should be changed to read

"... opportunities for computer-related crime ... exist."

Great is arguable, and I'm pretty sure, untrue. Exist is conformable to fact and not disputable.

3. Section 3, subsection d, paragraph 3 (D) reads

"report ... to Congress ... on ... the increasingly pervasive and widespread use of computers ..."

It should read

"report ... to Congress ... on ... the increasingly widespread use of computers ..."

Although, in another context, pervasive does not quite mean the same as widespread, in the context of the bill, the two words are denotatively identical. But pervasive has a somewhat pejorative connotation, unlike widespread, which is adequate for your meaning and is neutral as well. Pervasive should be struck so that Congress means that it is "interested" in the widespread use of computers for possible consequential problems, rather than it is "suspicious" about the pervasive use of computers.

4. Section c, definition of "use" reads

" ... or otherwise utilize ... memory functions of a computer"

Memory should be changed to storage, the preferable word that avoids unnecessary anthropomorphic connotations of memory. Also, utilize is an unnecessary latinized substitute for English use (see any usage dictionary). As a matter of fact, the entire clause

" ... or otherwise utilize ... of a computer" can be reduced to

" ... a computer"

with no loss of meaning since you have previously defined "computer" as including logical, arithmetic, and storage functions.

My article includes a copy of the bill in which I have pencilled in these changes plus corrections to what seem to be typos.

Sincerely yours

John K. Taber

John K. Taber

ON COMPUTER CRIME BILL S240

John K. Taber
609 Meadow Ave.
Santa Clara, Calif 95051

Home: [REDACTED] XXXX
Work: (408) 463-3182

ON COMPUTER CRIME BILL S240

Introduction	1
Computer Crime: Facts and Myths	2
Prison Programming	6
Outlaws Common Practices	10
Makes Felonies of Absurdities	12
May Be Abused	13
Conclusion	20
References and Notes	22
Appendix: Federal Computer Systems Protection Act	33

INTRODUCTION

I wish to bring to the attention of interested readers information about Senate Bill S240, now pending in Congress. This bill attempts to define and outlaw "computer" crimes. It is sponsored by Senator Ribicoff (D-Conn.). The bill was formerly known as S1766.

Senate Bill S240 consists of a preamble and three sections. The preamble claims that computer crime is a growing, serious problem difficult to prosecute under existing law, thus necessitating the bill. Section a attempts to outlaw any use of a computer for fraud; section b outlaws "intentional, unauthorized" use, access, or alteration of a computer, computer programs or data. Section c consists of definitions of terms. The bill covers government computers, computers for private entities with government contracts, computers used in banking and finance, and computers used by "any entity ... affecting interstate commerce." Penalty for violation of section a is 15 years and/or a fine of 2½ times the amount stolen; for section b 15 years or \$50,000 fine, or both.

The bill is dangerously vague and broad; it has potential for serious abuse; and it is largely unnecessary. It should be opposed.

COMPUTER CRIME: FACTS AND MYTHS

The rationale presented by the bill's preamble is not established. There is no evidence that computer based fraud and embezzlement are increasing. In fact, the loss from computer crime is insignificant. I say this well aware of sensational accounts of computer crimes in the mass media. Simply put, mass media accounts are grossly exaggerated or just myths. For example, newspapers widely reported the Security Pacific Bank theft in Los Angeles as a "computer" crime; in fact, it was not. The Pennsylvania RR boxcar thefts were reported as a "computer" crime; again, in fact, the thefts were not. The Equity Funding fraud, one of the largest ever, also was reported as a "computer" crime; this is very much disputed.¹

The Government Accounting Office found 69 cases of computer crime in the entire Federal Government, from information supplied to the GAO by many Government investigative agencies after a search of their files. Actually, however, there were only 66 cases; the Air Force had erroneously identified three cases as computer crimes that in fact did not involve computers in any way.² Nine cases involved no dollar loss, they were incidents such as privacy invasion. The total loss was \$2,161,413. The average loss was \$44,000, and the median, or typical, loss was \$6749.

In a study conducted by Stanford Research Institute, and based largely on newspaper articles, the dollar loss for 1975 was given as \$1.45 million. This includes the private sector as well as local and National Government. The total accumulated loss for the past

15 years was given as \$280 million. The average was \$450,000. Estimated annual losses vary wildly; \$100 million, \$300 million, \$160 million in 1985. In contrast, the estimated loss due to white collar crime in 1974 was \$40 billion.³ These figures are very questionable; there is something especially wrong with the average of \$450,000, more than ten times the GAO average; probably, the difference is due to the fact that it is based on amounts quoted in newspaper articles; but even if one accepts these figures blindly, the fact remains that computer crime losses compared to white collar crime losses are insignificant.

Furthermore, the incidence rate is insignificant. In 1975 there were 381 known incidents of computer "abuse" world-wide, since the advent of computers. Of these cases, 77 are verified, 218 cases have been assigned varying "levels of confidence" (ie, credibility weights as actually having occurred), and 86 are unverified.⁴ Some are suspected to be fictitious. This is an important point; many well known cases of computer crime, which have become part of our folklore, have never occurred; they are totally mythical, even if computer professionals widely believe and cite them.⁵ Even verification has dangers; Parker reports that two cases which were verified actually turned out to be fictitious. In other words, that figure of 381 "abuses", as small as it is, could well be much smaller, and must be treated with circumspection. But even accepting this figure tentatively, we are led to an "abuse" incidence rate of one case per year per 2000 computers. This is an insignificant rate.

It must be pointed out that these 381 cases are not all crimes - they include a large number of questionable uses of computers and odd incidents. Some don't really involve computers at all, for example, the stealing of check forms for forgery from the computer printer area. Of these cases, 145 involved fraud or theft (counting Equity Funding, 144 otherwise). A surprising number, 66, involved physical assaults on the computer, including four cases of the computer being shot, and one of a woman in France who beat up her CRT terminal with her high-heel shoe. Many cases are not crimes but are perhaps unethical. A good example is that of an instructor who used his school's computer to print 50 copies of campaign material in an election involving school issues. Others are student shenanigans with school computers, which most of the time do not involve criminal motives. Because of loose definitions and somewhat arbitrary classifications ("stealing" a password for example, is classed as theft) it is difficult to determine the number of real crimes out of the 381 "abuse" cases; it is about 210. They are false entry of records, fraud and embezzlement, theft, including theft of computer programs and theft of records, vandalism and sabotage. These are crimes already adequately covered by existing state and Federal laws.⁶ There are over 40 applicable laws at the Federal level alone. S240 is simply unnecessary.

There are other "estimates" that should be mentioned. One is that only 1/5 of detected "computer" crimes are reported to the authorities from fear of embarrassment. There is no evidence to support this contention. Furthermore, Federal regulations require

financial institutions to report all crimes. It seems to me unlikely that they don't, unless there is a massive breakdown in enforcement of banking regulations. If there is, a new law will hardly cure the problem. Another estimate is that only 1/100 of computer crimes is ever discovered. There is not one shred of evidence to support that figure; one would more profitably discuss the number of angels that can dance on the head of a pin.⁷

It may be argued that the use of the computer for fraud creates a unique sort of crime which requires its own criminal law. I doubt this; it seems to me that the use of the computer in fraud is equivalent to the use of the office adding machine or tub file. It is inconceivable that we need federal law to cover the case of the computer operator who in frustration shot his computer, or the woman who beat up her terminal. There is an ancient principle that holds that the law is concerned with serious matters, not with trivia. The appropriate sanction for cases like that of the instructor who misused the school computer is reprimand from his employer, or even dismissal, depending on the gravity of the case - but certainly not 15 years in Federal prison! The system programmer who without authorization plays tic-tac-toe on a computer should be beneath the notice of the law.

It is also argued that computer crimes are difficult to prosecute. This is nonsense. Quite the contrary in fact, convictions have been easy to obtain, sometimes where the prosecution was an unwarranted intrusion of Federal power into areas of state sovereignty.

In the Kelly and Palmer case in Philadelphia, Kelly and Palmer had used their employer's computer without permission in their own outside music business. The Federal prosecutor tried them for mail fraud for advertising their music. A conviction was obtained but the result of appeal is unknown to me. This is a clear case of unwarranted Federal intrusion into a state matter.⁸ In the Jones case, the U. S. Attorney complained at the Hearings that the judge would not allow a charge of forgery, which he attributed to the legal complexities caused by computers. He said that the judge's ruling implied that the computer committed the forgery, and thus Jones could not be charged with forgery. More likely, however, the legal complexities were caused by the fact that the forgery occurred in Canada where the U. S. prosecutor does not have jurisdiction.⁹ It would seem that the U. S. attorney blamed the computer for his own bungling of the indictment. Jones was convicted under the correct charges allowed by the court. In every known case in which real crime occurred, prosecutors have been able to secure convictions under existing law.

PRISON PROGRAMMING

The Dept of Justice, and other proponents, contend that computer crime is easy to commit and difficult to detect. For inexplicable reasons they seem to regard programmers with suspicion and some hostility. The FBI is afraid of "computer freaks", and a Time magazine article on computer crime, whose obvious source was the Dept of Justice, concluded with "Ideally, the first step in

securing a system would be to shoot the programmer." ¹⁰ This hostility is impossible to understand; studies of computer crime, as flawed as they are, agree that they are rarely perpetrated by the programmer (it is usually the data entry clerk or the managers). Apparently, this fear and hostility doesn't apply if the programmers are armed robbers, murderers, and forgers. The Dept of Justice's Bureau of Prisons runs a small but burgeoning data processing service employing convicts in at least six Federal prisons. ¹¹ Customers include the Dept of Defense, Dept of Agriculture, Internal Revenue Service, the Bureau of Prisons itself, and the National Endowment for the Humanities. The Dept of Agriculture has even located its new computer center in Kansas City, Missouri just to be close to the convict programmers incarcerated in Leavenworth. Gross earnings in fiscal year 1976 were just shy of one million dollars, and must be well over that today. Federal Prison Industries Inc. claimed net profits of about 15 percent for contract data processing services. Data entry services are provided for the Navy's supply system by female offenders in Alderson, W. Va. and Terminal Island, Calif. Serious COBOL programming is provided by Leavenworth inmates for the Agricultural Stabilization and Conservation Service of the Dept of Agriculture. These programs form part of the general ledger and accounting programs of the Dept of Agriculture, and affect the disbursement of funds. The same Leavenworth convicts have reportedly written unspecified programs for the IRS. Indeed, there were rumors at one time, apparently

unfounded, that the convicts learned enough about the IRS computerized tax return system so that they were filing fraudulent returns that escaped detection by the IRS computers. I stress, however, that these rumors appear to have been unfounded. Furthermore, future prison business can only grow, provided that enough prisoners can be found willing and able to program. The GSA, no doubt at the urging of the Dept of Justice, promulgated Federal Procurement Regulation 1-5.402 on Dec 2, 1974. This regulation requires all Federal agencies to give priority to the Federal Prison Industries, Inc. over private industry for all data entry and programming services. The agencies are required to pay the going commercial rates with perhaps an incentive deduction.

There is something clearly insane here. On the one hand, the Dept of Justice asks for a broad, dangerous law because it says computer crime is so easy to commit and so difficult to detect. On the other hand, the Dept of Justice sees nothing wrong with prisoners convicted of serious crimes programming accounting applications, and indeed the Dept even attempts to increase such activities through Federal regulation. The insanity is called schizophrenia.

The truth is, there is nothing wrong with the prisoners writing programs. Computer crime is not easy to commit, and the Bureau of Prisons is living proof. It is the one good job training program in the entire Federal prison system. The qualified convicts learn a useful trade, unlike the usual prison job training, such as broom and mail sack making, and are quickly hired on release

in meaningful, well-paid jobs. As one would expect, the recidivism is extremely low. In other words, I do not want this discussion of prison programming misunderstood; the point to be made is that the Dept of Justice itself gives the complete lie to contentions in favor of the Ribicoff bill. I would suggest, however, that FPR 1-5.402 be rescinded to avoid the possibility of abuse. Many prison programmers are worked over 14 hours a day by the admission of the authorities. Growing business may tempt prison staff to coerce unwilling or unsuited prisoners into programming. Also, it may be wise to redirect programming away from high priority work to low priority work that normally would not get done due to lack of assignable personnel. This would remove any temptation that might exist on the part of Government agencies to exploit what amounts to slave labor while still keeping a worthy program going.

OUTLAWS COMMON PRACTICES

Section b of the bill is too broad. It fails (in fact, it doesn't attempt) to distinguish felonious misuses of computers from misdemeanor misuses or from ethically questionable uses. I will address the "unauthorized" use, which is neither felony nor misdemeanor.

"Unauthorized" use of a computer is widespread among programmers. Programmers on occasion use their employers' computers to play games like tic-tac-toe, Adventure or Star Wars. They draw tabby cat calendars and pinup girls. They have discovered that certain combinations of nonsense characters on the 1403 line printer generate musical tones, and I know a programmer who played "She'll Be Comin' Round the Mountain" on the printer; he also used judiciously timed page ejects to create a drum beat accompaniment. Programmer ingenuity is amazing. They use the computer to balance their checkbooks, chart the misfortunes of their stocks, and figure their mortgage tables. They write "unauthorized" programs that have little earthly use, out of curiosity, like the knight's tour of the chessboard, or a base-256 multiplier. Sometimes, an "unauthorized" program proves useful, and travelling the programmers grapevine, becomes unofficially adopted at computer centers all over the world. This play and incidental personal use is without pecuniary motives. All of it is a serious crime under section b.

There may be some who would argue that such play should be forbidden; the computer is not a toy, but a very expensive asset. Such games in effect steal time and resources from their rightful owners. This argument has merit, I am not trying to condone unethical behavior with the excuse that everybody does it. But Senate Bill S240 is a radical "solution" to this problem - if it is a problem. Imprisonment for 15 years is a sanction out of all proportion to the offense. The bill is improper intrusion into an area where there can be no legitimate public policy interest - employer sanction is adequate and proper. Also, employer attitudes vary widely. Some flatly forbid non-business uses of their computers, and what is more, police machine usage to enforce the ban. Others forbid it in theory, but allow it in practice, and indeed even wink at it. Others allow it as a sort of fringe benefit. For many companies, the question has never occurred to them.¹² Thus, an act committed on one computer would be perfectly legal, and may even win the programmer commendations, while committed by the same programmer on another computer would cause his imprisonment. This bill cannot ever be equitably enforced.

In any case, great care must be exercised in forbidding such uses; Eliza, for example, is one such game, yet it is a classic in artificial intelligence research. Many "games" in fact provide great insight into computer programming and are of professional benefit. I suspect that in many areas of science, mathematics, and computer science it will be impossible to distinguish between "unauthorized" use and research. I suspect that researchers will

find this bill intolerable.

The bill does not address the problem of who may authorize what uses of the computer. Presumably, the authorizer is the employer, which leads to the absurdity that the Equity Funding fraud would not violate section b because the company officers authorized the use of the computer in perpetrating the fraud. The question of who may authorize what, is not idle. Commonly, "employers" are "users" and do not own either the hardware or the software; these are rented, and the owner does not relinquish rights of ownership by renting them to the user. Yet it is common practice for the user to alter rented code (and even hardware) without authorization from the rightful owner. In fact, the owners generally prefer that the user doesn't modify software because of the maintenance problems it creates. Thus, section b, which makes unauthorized alteration of computer programs a felony, will force wholesale renegotiation of contracts. There is no good reason to change this common industry wide practice.

MAKES FELONIES OF ABSURDITIES

The definition of computer is too loose; "computer means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses.." This definition would include, and is apparently meant to include, pocket calculators and even some digital watches. ¹³ The fact is that

microprocessors enjoy wide application today in all sorts of gadgets. Thus, under this bill, a secretary who uses the office typewriter with a microprocessor in it to type a personal letter, and the office worker who plays the "shell oil" calculator joke on his calculator at work, when presumably they are not authorized to do so, are felons that may be imprisoned for 15 years. I doubt very much that this definitional problem can ever be overcome. We in the industry cannot agree on a definition of computer for technical purposes, let alone legal.¹⁴

MAY BE ABUSED

I most strongly protest that this bill has dangerous potential for abuse. First, the bill is a serious threat to privacy. Second, there is an obvious danger of jailing programmers (and all other computer users) for bagatelles.

The reader must realize that record keeping is the most important use of computers today from a social point of view. Most record keeping is computerized, and virtually all records soon will be. This bill, because it is so broad, gives legal access to most records to the FBI, under their investigative powers, which it never had before. This point was made by Senator Biden at the hearings on this bill. It is worth quoting:

"I know that there is a good deal of criticism and concern about abuse of power by (the FBI, the CIA, and

our security industry)... We are going to be turning to these agencies and saying 'We are going to broaden your jurisdiction now. We are going to allow you legally to get into a number of data banks that you did not have access to before' ... Your legislation is very broad. As I read it, just about any computer in America will be accessible for the first time to investigation by a major Federal law enforcement agency." ¹⁵

Precisely. The point is undeniable, and Senator Percy, to whom Biden was speaking, did not deny it. Senator Percy allowed that S240 was not a panacea, and when Biden pressed the point, Percy expressed pious hopes that a privacy bill, "vitally needed", (but not enacted yet) would help prevent abuse. Nor did Senator Ribicoff deny it, nor yet the Justice Department which had requested the bill in the first place, nor did the FBI spokesman. I sincerely hope that the Congress would reject this bill on this point alone.

The second potential abuse is the arbitrary jailing of programmers for bagatelles. As has been pointed out, "unauthorized" use of computers is widespread. The bill will not change this fact. Most will be unaware of the law. Second, whether correct or not, they do not feel that their personal use of computers is wrong, so long as it is not for material gain. Third, even if some become aware of the law, they will simply disbelieve that it applies to their "unauthorized" use of computers - their feeling is that that

is too absurd. Generally speaking, computer professionals are technically oriented and do not know or care how laws and sausages are made. The result will be that most programmers (and many other computer users) will be unprosecuted felons, vulnerable to abuse. This is too much discretionary power to give law enforcement. While some discretion is necessary for effective law enforcement, modern American history does not make happy reading in the enforcement of broad laws. The FBI has abused its powers; I cite its abuses of the Mann Act and the Dyer Act. It has acted illegally in searches and seizures; why legalize it? Prosecutors have out of sheer muddle-headedness, not to mention ambition, jailed people who should never have been charged.

But, of course, will this specific law be abused? The Dept of Justice said it would prosecute only cases in which the Federal Government has a compelling interest. This is cold comfort; it means only that if a programmer is jailed for playing computer tic-tac-toe, why it must be presumed that the Government had a compelling interest.¹⁶ It should be noted that nowhere does either the FBI or the Dept of Justice explicitly promise not to prosecute the programmer who plays tic-tac-toe or draws a calendar, even under direct questioning on the point:

BIDEN: Let us level with the public. Let us acknowledge to them, by implication at least, that we are not going to prosecute that particular person ...

FINNEY (Dept of Justice): The Snoopy (calendar) was our case.

BIDEN: Yes. Acknowledge that we are not going to prosecute Snoopy and do not leave the possibility of abuse. ¹⁷

Finney responds then for several pages, mentioning the good sense of the FBI and the Dept of Justice, and claiming that trust is needed, but he does not give the acknowledgement asked for and he avoids explicitly committing to not prosecuting these bagatelles. ¹⁸

Will computer users be jailed for bagatelles? The probability is grim. Past performance is one indication, but even more important is impetus. Computer crime does not exist, it is a misnomer applied to several crimes that may or may not involve computers; on the whole, record keeping crimes. But it is a new, glamorous crime, currently sensationalized by the media. Even Dick Tracy is fighting computer crime. ¹⁹ Currently, Penthouse is planning an article on it. Computer crime suffers great publicity which creates the impression of a widespread problem, and generates pressure for the prosecution of computer criminals. However, there are scarcely any, except the programmer playing tic-tac-toe. The prosecutor, trained for and assigned to computer crime, will have to be content with the programmer if he is ambitious for his career.

The reader may think it unlikely that a judge would permit prosecution of the tic-tac-toe player. Unfortunately, the reader is mistaken; the judge will have little choice. Senator Ribicoff, on reintroducing the bill as S240, said in the Congressional Record

that this type of "playing around" is the same type of activity that enables computer crime. He cited the specific example of a Dept of Agriculture employee at the Washington Computer Center who permitted his children to play computer games on the WCC computer. There is scarcely a programmer in the country who hasn't done the same. But the same employee had also used the WCC computer for his own outside consulting business. The drift of Senator Ribicoff's contention is that the main purpose of the bill is not to jail programmers for "playing around"; but to change the language of the bill to accommodate "playing around" would seriously weaken the bill. Therefore, if a programmer falls afoul of the language, too bad. He shouldn't be "playing around" anyway.²⁰ This is more than a Senator's mistake. Trial judges, when attempting to apply a new law in a doubtful case, consult the legislative record to divine the legislator's intent. Unless there are constitutional grounds, the judge is required to respect that intent, and I remind the reader that the Constitution does not forbid bad laws, only certain bad laws. Senator Ribicoff was clearly instructing trial judges as to his intent. Thus if this bill becomes law, the judge must permit the trial, which will be limited to the factual determination of whether or not the programmer played

-17-

tic-tac-toe without authorization, and intentionally. We hope that the programmer will not receive a severe sentence, but even here the judge may be very limited. Senate Bill S1437, the successor to SB1, may become law soon. This bill limits the judge's sentencing discretion to a formula of plus or minus 25 percent of the nominal sentence. The programmer must receive a minimum sentence of 11 years and may receive as much as 19.

For some time now, the FBI has been training prosecutors and law enforcement personnel on computer crime. The FBI conducts a one week course, the more common course, and a four week course at Quantico, Va. The one week course has graduated over 500. Mr. Henehan, of the FBI said in testimony that "there is a reluctance on the part of both the prosecutors and the investigators to get into these cases (that is, computer crime). We find that through training they are much more anxious to accept a case." It seems that this course generates enthusiasm for prosecuting computer crimes.²¹ I don't think there is much else a one week course could do for people unfamiliar with computers. Also, the FBI thinks that it will need 200 more special agents, 45 more accountant technicians, and 10 auditor-computer specialists. What this means is that a lot of people are being geared up to prosecuting and investigating computer crimes, a glamorous new area, in which unfortunately there is little to do, except for programmers playing tic-tac-toe.

Thus, I think the chances for abuse are enormous. Our only protection so far is the FBI's and the Justice Dept's promises that we can trust them, without, however, any explicit commitment.

CONCLUSION

Senate Bill S240 is an ill-formed and dangerous law that must be rejected. Minor flaws can be corrected no doubt, but the bill is fundamentally flawed. For example, one could correct the bill's English; it uses "access", a noun in Standard English, as a verb for no apparent reason. This usage is computer jargon that the Congress should not inflict upon the U. S. Code. Also, section a, which duplicates existing fraud laws (but with conflicting punishment) can be eliminated as unnecessary. But the fundamental problem is that it defines an abstraction, "computer crime", as a crime rather than specific acts. Compare "computer crime" with "filing cabinet crime" to make this flaw apparent. Computer crime (or filing cabinet crime) beclouds specific criminal acts, and non-criminal acts, with a trope drawn from the instrument of the acts. It is true that one may commit murder with a filing cabinet by dropping it from sufficient height on a victim, and one may tamper with records using a computer to perpetrate a fraud. Nevertheless, the crime is murder, not unauthorized use of a filing cabinet, and fraud, not unauthorized access of a computer.

Criminal law as I understand it, is pragmatic; its concern is concrete acts that have active, stark verbs to describe them; steal, murder, defraud, vandalize. There is a corresponding stark noun to name the doer of the active verb; thief, murderer, defalcator, vandal. Let us not now create out of latinate English, the adverbial crime, "access without authorization", of which the sense at least is passive voiced. It lacks a clear noun to name the doer.

REFERENCES AND NOTES

X Senate Committee on Government Operations. Staff Study of Computer Security in Federal Programs. Committee Print. 95th Congress, 1st Session, Feb. 1977.

Senate Committee on Government Operations. Problems Associated with Computer Technology in Federal Programs and Private Industry. Computer Abuses. Committee Print. 94th Congress, 2nd Session, June 1976.

X U. S. Senate. Hearings before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary. Federal Computer Systems Protection Act. (S1766). 95th Congress, 2nd Session, June 21 and 22, 1978.

Parker, Donn F.; Nycum, Susan; Oura, Steven. Computer Abuse. Stanford Research Institute Report (NTIS # PB 231-320/AS). Nov 1973.

Parker, Donn B. Computer Abuse Assessment. Stanford Research Institute Report, NSF Grant MCS 76-09183. Dec 1975.

Parker, Donn B. Computer Abuse Perpetrators and Vulnerabilities of Computer Systems. Stanford Research Institute Report, NSF Grant MCS 76-09183. Dec 1975.

- ✓ Parker, Donn B. Crime by Computer. Charles Scribner's Sons. New York. 1976
- ✓ Loeffler, R. M. Report of the Trustee of Equity Funding Corp of America. Oct 31, 1974.
- ✗ "Introduction of S240 by Mr. Ribicoff", Congressional Record. Vol 125, No. 7. Jan 25, 1979. pp S709 - S726.
- ✓ U. S. Chamber of Commerce. A Handbook on White Collar Crime. 1974
- ✓ Federal Prison Industries, Inc. Annual Report, FY 1976.
- ✗ "Computer Capers", Time, Aug 8, 1977; pg 53.

1. The boxcar thefts were due entirely to manipulation of manual records. R. M. Loeffler denies that the computer was an essential part of the Equity Funding fraud. The Security Pacific Bank theft in no way involved computers. The culprit, Rifkin, obtained the bank's password by observing the teletype operators in the transfer cage, a place to which he should not have been given access. He then telephoned the order to transfer funds from Security Pacific to a bank in New York by impersonating a bank officer and supplying the correct password. Amusingly enough, Rifkin used the wrong Security Pacific account number in his first attempt; he then obtained the correct account number from bank officials and then repeated the phone call, this time successfully. Oddly, Parker is including this case as "computer abuse" because the transfer cage was located in the computer room (personal communication).

2. The GAO report is included in Problems. The correction to the GAO report is from a statement by Joseph F. Welsch, Deputy Assistant Secretary of Defense for Management Systems, Dec 3, 1976, in Computer Security, pg 149. He also mentions that one Army case out of 16 involved conflict of interest on the part of computer management personnel rather than computer crime; however, it is not clear whether this case was included in the GAO study or not. Presumably, it was.

3. These figures are from several sources. \$280 million is from Parker's testimony in Hearings. \$160 million is quoted in Computer Abuse Assessment from an Institute for the Future (Menlo Park, Calif) report prepared for Skandia Insurance, Sweden. \$100 million and \$40 billion, also quoted in Assessment, come from Handbook. \$1.45 million and \$450,000 are both from Assessment. \$300 million, cited by Time in an article on computer crime and the Ribicoff bill, Aug 8, 1977, probably comes from Crime by Computer; it is pure guess, based on unjustified assumptions that 100 cases would be reported in a year and that these are 15 percent of all computer related crimes in a year, at the rate of \$450,000 per case.
4. Assessment, pg 10.
5. The round-off fraud is an example. In this fraud, the programmer accumulates remainders after round off into his account instead of distributing the remainders among all accounts. With many accounts and over a period of time, this fraud could result in a tidy sum. However, the possibility of fraud in round offs was so well known long before computers and so well guarded against that it is practically impossible for it to succeed. Another clear example of myth is the

Zwana/Zzwicke story where the programmer shortchanges accounts and deposits the shortchange in a false, last account. In one version of the story, SRI case number 71319N, the false account is a commission account for a fictitious salesman named Zwana. In another version of the story, the false account is a customer named Zzwicke, reported for real with a straight face by Brandt Allen in Harvard Business Review, Jul-Aug 1975. In all versions of the story, the fraud is discovered when Marketing pulls the first and last names for a promotional campaign. Wasn't that programmer surprised! The provenance of the story is second generation computers that used punched card and tape files - that is why the false account is last. I strongly suspect that the MICR stories in the SRI cases, and mentioned by proponents of S240, are also myths. There are many such myths, too numerous to mention.

6. Applicable Federal laws are listed in Computer Security. There is a legal nicety involved in the theft of programs and computerized records. Generally, the theft does not involve asportation; there is no "taking" in the legal sense because the owner is not deprived of the program by the theft. Instead, the theft involves a wrongful copying. Thus the thief cannot be charged with larceny (common law theft) but must be charged instead with theft of trade secrets or

copyright violation (statutory charges). There are some who feel that the law should be modified to support common law theft charges in these cases. It is a minor issue; I fail to see how it matters whether the thief is punished for larceny theft or trade secret theft.

7. 1/100 cited by August Bequai, Computer Security, pg 185, attributed elsewhere to the Commerce Dept, Hearings, pg 18. Bequai, adjunct professor of law, American University, is the principal author of S240, along with Phil Manuel of the Senate Government Affairs Committee staff. 1/5 quoted skeptically by Biden, Hearings, p 37.
8. Time, Aug 8, 1977, pg 53. I think that the conviction was overturned on appeal because this case has dropped from mention by the proponents of the bill, yet it was the shining example in the Time article on the Ribicoff bill. The Seidlitz case, involving the theft of a computer program is another intrusion into a state matter, although here the prosecutor claims that the local police requested Federal intervention (Hearings, pg 88). Nevertheless, it was a state matter.
9. Hearings, pg 88.
10. Time, Aug 8, 1977; pg 53.

11. In FY 1976 the prisons were Alderson W. Va.; Lexington, Ky.; Miami, Fla.; Terminal Island, Calif.; Fort Worth, Tex.; and Leavenworth, Kan. By now there are probably other prisons providing contract data processing services. Also, one should not overlook contract programming services provided by many state prisons; Minnesota had a bill in Congress to allow interstate commerce of prison written computer programs: see Hearings before the House Education and Labor Committee, 94th Congress, 2nd Session, on Job Training, GPO number Y4.Ed 8/1:p37. Details on type and extent of programming are taken from Computer Security and Annual Report.

12. IBM prohibits non-business uses of their computers and conducts internal audits to ensure compliance.

If Hewlett-Packard has a ban, their programmers are unaware of it. Many smaller firms too numerous to mention allow non-business use as a sort of fringe benefit. An example of an unofficial program is DEBE (Does Everything But Eat). It is a useful utility program written without specific authorization, and is in use wherever there are IBM computers. There are many others like DEBE.

13. When it was pointed out to the staff members of the Govern-

ment Affairs Committee, who helped draft this bill, that their definition of computer includes trivia like pocket calculators, they indicated that they meant to. They posited a bizarre illustration of a mortgage applicant tampering with a bank officer's calculator to make the payments fraudulently benefit the applicant (private communication with Parker). I don't know how they expected the applicant to do this; perhaps by weaving a circle thrice about the banker while intoning abraxas.

14. Parker attempted to get several computer scientists to define "computer" for Senate bill S66, State Senator Cusanovich's little Ribicoff bill, introduced Dec. 1979 in Calif. Agreement was impossible to achieve. (private communication with Chuck Mobley, Senator Cusanovich's staff consultant). The state bill, by the way, was not well received by the State Senate Judiciary Committee, Feb 27, 1979. The Committee Staff's digest pointed out many serious defects. The bill was "put over", that is, returned to the sponsoring Senator with directions to rework it. It is not expected back before April or May.
15. Hearings, pp 24 - 25. Also see p 36.

16. Congressional Record, p S715, John C. Keeney, Acting Assistant Attorney General. Also, FBI in Hearings, pg 36.
17. Hearings, pg 91. The choice of Snoopy calendars as the generic term for this type of "playing around" is due to Donn Parker of SRI and is poorly chosen. Years ago, Charles Schulz 's attorneys requested the industry to end the making of Snoopy calendars by their computer personnel because the practice infringed on Mr. Schulz 's copyrights. Management agreed, and suppressed the practice. I have not personally seen an illicit Snoopy calendar since about 1970. I request all participants in discussions on the computer crime bill to refrain from using this example so as to avoid unnecessarily alarming Mr. Schulz . If a generic term is needed, I suggest tic-tac-toe, or the contemporary rage "Adventure", written by computer scientists at MIT and Stanford's Artificial Intelligence laboratory.
18. Hearings, pp 91 - 95.
19. Dick Tracy seems to be out-and-out Dept of Justice propaganda.
Contrast:

Computer users are curiously ambivalent about security. Consider the business man who would never leave his checkbook lying on top of his desk ... This same business man will purchase a multimillion dollar computer ... without an audit as basic as a cancelled check -

will place a computer terminal on top of the desk unattended. (Richard L. Thornburgh, Nixon's Assistant Attorney General, Nov 15, 1976, Computer Security, pg 228.

and this from Dick Tracy, Jan 28, 1979:

DETECTIVE SAM: Sir, do you leave your billfold out on your desk, when you go to lunch?

WALTER PREMIUM (Business man, president of Equity America Life, whose computer is a "\$1,000,000 loss" due to a shotgun fired in its chips, "not just the computer, but data too"): What? Certainly not!

DETECTIVE SAM: Well, doesn't a multi-million dollar computer complex deserve as much consideration as a billfold? During the lunch hour here, only a secretary and a computer programmer stood between a MANIAC and your elaborate computer system.

Thornburgh, by the way, is now Governor of Pennsylvania.

20. Congressional Record, pp S722 - S725. Throughout this lengthy contention, Ribicoff stresses government computers, over which the Congress, as employers, may be presumed to have a rightful interest in their use for non-business purposes. Only at the end, in one brief clause, does he mention computers of "certain organizations involved in interstate commerce." The impression created by his emphasis on Federal computers is disingenuous: Senator Ribicoff is certainly aware that the bill covers computers of "entities affecting interstate commerce", meaning virtually all computers in the private sector, not just "certain" interstate instances.

21. Hearings, pg 35.

QUESTIONS OF SENATOR BIDEN AND RESPONSES OF THE FBI



UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

WASHINGTON, D.C. 20535

March 19, 1980

Ms. Kathy Zebrowski
Counsel
Subcommittee on Criminal Justice
United States Senate
Committee on the Judiciary
Washington, D. C. 20510

Dear Ms. Zebrowski:

Director Webster has requested that I respond to your letter dated February 25, 1980, concerning Senate Bill S. 240. In your letter you asked the following:

- (1) What has been the role of the FBI in investigating crimes involving computers?

The FBI currently does not have investigative jurisdiction in computer crime matters, however, we do encounter some investigations of this type in matters such as bank fraud and embezzlement, interstate transportation of stolen property, theft of Government property, and fraud by wire, which are currently within the FBI's investigative jurisdiction. These cases are received during the normal course of business. Because of the lack of a Federal statute involving computer crime, some of these crimes are prosecuted when a Federal violation can be identified which, in most instances, is very difficult.

In your second question, you asked:

- (2) In what ways can the FBI assist in Federal prosecutions of computer crimes as defined in S. 240, as amended?

The FBI can assist in Federal prosecutions through its available trained resources. Since 1975, the Bureau has been training its investigators in handling computer fraud investigations. Currently, we have trained over 500 Agents in a one-week course enabling them to handle frauds involving automated accounting systems. In addition, we now have over 100 Agents who have completed a four-week course enabling them to handle sophisticated computer frauds. Also, the FBI has a computer dedicated to computer fraud training at the FBI Academy. Our investigative resources are limited but we do have the necessary expertise available to utilize this new investigative tool in attacking the sophisticated white-collar crime encountered in computer frauds.

Sincerely yours,

Francis M. Mullen, Jr.

Francis M. Mullen, Jr.
Assistant Director
Criminal Investigative Division

Resolution of the ABA

AMERICAN BAR ASSOCIATION

SECRETARY
F. Wm. McCalpin
Room 1400
611 Olive Street
St. Louis, MO 63101

1155 EAST 60TH ST., CHICAGO, ILLINOIS 60637 TELEPHONE (312) 947-4016

September 11, 1979

Honorable Joseph R. Biden, Jr.
Chairman, Subcommittee on Criminal Justice
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Re: Jurisdiction Over Crimes Committed
Against or Through Use of Computers

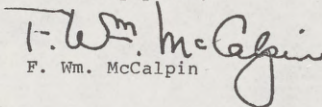
Dear Mr. Chairman:

At the meeting of the House of Delegates of the American Bar Association held August 14-15, 1979 in Dallas, Texas the attached resolution was adopted upon recommendation of the Section of Criminal Justice. The action taken thus becomes the official policy of the Association in this matter.

This resolution is transmitted for your information and whatever action you may deem appropriate. If hearings are scheduled on the subject of this resolution, we would appreciate your advising Herbert E. Hoffman, Director of the American Bar Association Governmental Relations Office, 1800 M Street, N.W., Washington, D.C. 20036, (202) 331-2210.

Please do not hesitate to let us know if you need any further information, have any questions or if we can be of any assistance.

Sincerely yours,


F. Wm. McCalpin

FWM/LAD/kay
Attachment
3771A/0413C

cc: Richard E. Gerstein, Esquire
Chairman, Section of Criminal Justice
Herbert E. Hoffman, Esquire

BE IT RESOLVED, That the ABA support legislation to establish federal jurisdiction, concurrent with state jurisdiction, over certain offenses committed against, or through the use of computers, computer systems or computer networks;

BE IT FURTHER RESOLVED, That the proposed federal concurrent legislation reach:

- (a) the use or attempted use of a computer, computer system or computer network to obtain money, property or services by means of false or fraudulent pretenses, representations or promises;
- (b) intentional, unauthorized accessing for the purpose of alteration, damage, destruction or theft of a computer, computer system, computer network or any computer software, program or information contained therein;
- (c) intentional, unauthorized interception of nonaural communications by wire or radio between computers, computer systems, or computer networks;

BE IT FURTHER RESOLVED, That legislation creating concurrent federal jurisdiction over offenses committed against or through the use of computers, computer systems or computer networks require the Attorney General, in consultation with state and local enforcement authorities, to publish guidelines for the exercise of that jurisdiction by the United States;

BE IT FURTHER RESOLVED, That legislation denominating federal offenses committed against or through the use of a computer or computer systems or computer network should:

- (a) preclude the charging of a federal offense based upon the same facts except for proof of an element involving a computer, with a charge brought under the computer crime statute;
- (b) provide for gradation of offenses and a graduated scale of penalties consistent with ABA policy on the sentencing scheme of the proposed Federal Criminal Code, with a sanction not to exceed five years imprisonment or \$50,000 or both; and

BE IT FURTHER RESOLVED, That additional study be undertaken to find solutions to the procedural and evidentiary problems that impede the detection and prosecution of computer crimes under existing law.

REPORT IN SUPPORT OF RECOMMENDATIONS

The Subcommittee on Criminal Laws and Procedures of the United States Senate Judiciary Committee held hearings on a proposed Federal Computer Systems Protection Act (S. 1766 - 95th Congress) during 1978. In a letter to the Criminal Justice Section, Senator Joseph R. Biden, Jr., Subcommittee Chairman, requested written comments by the ABA for Subcommittee consideration without further hearings. No action was taken on S. 1766 by the 95th Congress and the bill died at the close of the legislative session. Senator Abraham Ribicoff (R-CT) and twelve cosponsors introduced a slightly modified version of the Federal Computer Systems Protection Act proposal (S. 240) in January, 1979 (S. 240 attached).

The Section of Criminal Justice recommendations are based on a report submitted by the Section's Committee on Economic Offenses and Complex Criminal Litigation Problems in support of federal computer crime legislation. The Section takes no position on the technical computer definitions contained in the proposed Act.

Pending Legislation

The bill proposing the Federal Computer Systems Protection Act of 1979, S. 240, intends "to amend Title 18 of the United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions and entities affecting interstate commerce."

Section 2 of S. 240 details the need for legislation, highlighting the growing problem; the high cost to the public; the impact of this type of crime on federal programs, financial institutions and interstate commerce; and the difficulty of prosecuting computer related crime under current federal criminal statutes.

Section 3 adds a new section to Chapter 47 of Title 18 U.S.C. entitled "1028 Computer fraud and abuse." The critical portions of this new section are:

"(a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, computer system, computer network, or any part thereof which, in whole or in part, operates in interstate commerce or is owned by, under contract to, or in conjunction with, any financial institution, the United States Government or any branch, department, or agency thereof, or any entity operating in or affecting interstate commerce, for the purpose of --

"(1) devising or executing any scheme or artifice to defraud,

or

"(2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretenses, representations or promises, shall be fined a sum not more than two and one-half times the amount of the fraud or theft, or imprisoned not more than fifteen years, or both.

"(b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network described in subsection (a), or any computer software, program or data contained in such computer, computer system or computer network, shall be fined not more than \$50,000 or imprisoned not more than 15 years, or both."

As proposed by S. 240, 18 U.S.C. § 1028(c) will set forth the controlling definitions under the Act, including definitions of "computer systems" and "computer network" that are particularly far reaching in scope.

The Scope of Proposed Federal Jurisdiction

Some question the need for federal legislation that embraces a long list of offenses already proscribed by existing federal statutes (e.g., Mail and Wire Fraud, Interstate Transportation of Stolen Property and Fraudulent Documents etc., embezzlement and the various larceny statutes). The Attorney General in a letter to Senator Biden dated September 21, 1978, estimates and reports in part ". . . As reflected in the testimony before the Committee, there are no less than 40 Federal statutes on the books that conceivably might impact on computer fraud and abuse . . ." but refers to "existing ambiguities" which hinder or prevent the application of those statutes. Apart from the "ambiguities" reportedly caused by technical definitions, the principle justification for the apparent duplication of federal jurisdiction proposed in S. 240 is the deterrent effect of a single statute proscribing the use of a computer as an instrumentality of the offense. Direct Congressional statements of federal government authority to investigate and prosecute have improved federal law enforcement effectiveness and deterrence in the past. The wire fraud statute, 18 U.S.C. § 1343, for example, was enacted to discourage confidence swindles in which the interstate and foreign wires were used to further or accomplish the fraud.

It is important to note that some computer offenses are not encompassed by S. 240. The principle omission is theft of the unusual assets of the computer -- computer software, data and services. Prosecutors will also be forced to rely on judicial interpretation, similar to securities laws and mail fraud statute interpretations, to make the Act's language "devising or executing" reach computer "cover-ups" and "lulling."¹

Concurrent Federal Jurisdiction

Although federal computer crime legislation proposed to Congress creates potential problems in federal-state law enforcement relations by extending federal authority into areas of enforcement traditionally within the jurisdiction of state and local authorities based on the means used to accomplish otherwise wholly intrastate offenses, the position of the Attorney General is revealing on this point. In a letter to Senator Biden he states ". . . (1) As we indicated during our testimony, while the proposed statute may provide for expansive jurisdiction, it is not our intention to prosecute all conceivable violations. We are nevertheless, of the view that to reach all the instances of computer fraud and abuse which would be appropriate for Federal prosecutions and, in view of the uneven capabilities of state authorities to deal with the problem, broad jurisdiction would be highly desirable." (emphasis supplied)

The federal government is currently attempting to prioritize federal law enforcement efforts by seeking close cooperation from state and local agencies. While the language of the proposed Act does not constitute legal preemption, it can be argued that de facto preemption will take place if the federal government is given authority to "select" for prosecution cases that are traditionally considered local in character, unless the Attorney General develops guidelines for the exercise of federal jurisdiction over computer offenses in consultation with state and local prosecutors. Those guidelines should respect the capability of metropolitan prosecutors and state attorneys general with large, well-equipped economic crime units to investigate and prosecute major computer thefts and frauds. They should reflect policies consistent with the Department of Justice's stated intention to decline prosecution in the bulk of bank embezzlement cases (those involving less than \$5,000) in favor of state prosecutions, without regard to the use of computers in committing those embezzlements.

Published guidelines governing the exercise of federal jurisdiction over offenses committed against or through the use of computers can limit federal preemption to instances where required by the objective inability of local authorities to combat computer crime. The recommendation that published guidelines be required contained in the third Resolved clause of the Section of Criminal Justice recommendations is consistent with the position taken by the

¹ Many experts consider the famous Equity Funding case to have been a computer cover-up case, because the actual fraud was accomplished before the computer came into the scheme.

House of Delegates at the 1979 Midyear Meeting in adopting a Joint Substitute Resolution on the codification of federal criminal law.²

Charging and Punishment

In 1975, The Association adopted the position that "the several jurisdictional bases should be removed from the definitions of the substantive crimes, where they are now found in Title 18." The Criminal Code Reform Act of 1978 legislation (S. 1437) that passed the Senate in January, 1978, which would have separated the jurisdictional bases from the substantive offense, attempted to achieve the reach of current federal mail fraud and wire fraud statutes while obviating the most frequent criticism of current law -- pyramiding of offenses. Legislation introduced in the United States Senate thus far (S. 1766-95th Cong.; S. 240-96th Cong.) is inconsistent with the Association position on recodification of federal criminal law. In the absence of criminal code reform, however, legislation should be enacted in Title 18 that confers federal concurrent jurisdiction over certain computer-related offenses. The computer crime statute should preclude the charging of a federal offense based on the same facts except for proof of an element involving a computer, with a charge brought under the computer crime statute to avoid the pyramiding of offenses.

Although the Section of Criminal Justice believes that the need to deter both professional swindlers and amateurs or first offender "computer freaks" justifies a clear statement of federal law enforcement authority to investigate and prosecute computer crime, the Section believes that a sanction that includes 5 years imprisonment provides an adequate deterrent and represents an appropriate outer limit of sentence severity. Legislation pending before Congress prescribes a 15-year maximum term of incarceration without any structure of gradation to guide the exercise of sentencing authority. Fifteen years is overly severe and inappropriate. The broad undifferentiated range over which sentencing discretion would be exercised under that legislation conflicts with Association positions on structuring sentencing discretion and should be disapproved.

² "3. The Association makes the following specific recommendations with respect to codification legislation:

"(a) Concurrent Federal/State Jurisdiction. The Association expresses concern about the expansion of federal criminal jurisdiction over subjects within the traditional police power of the states. Accordingly, the Association

- "- recommends that codification legislation refrain from creating new federal offenses in situations now covered under state penal statutes absent a clear showing in the particular instance of a compelling federal interest;
- "- supports the proposal in the Brown Commission Report relating to publication of criteria for exercise of federal enforcement authority in cases of concurrent federal and state jurisdiction; and
- "- supports the proposal in that Report for the application of double jeopardy provisions to prosecutions in different jurisdictions."

Procedural and Evidentiary Problems

The proponents of S. 240 and its predecessor, S. 1766, contend that it facilitates detection, investigation and prosecution of computer crime. This, however, is an overstatement. The Attorney General also comments: "Use of traditional and prosecutive techniques for gathering evidence, such as immunity grants, grand jury inquiries, and search warrants, would be just as effective in this area (computer crime) as in dealing with any other white collar illegalities. However technical problems associated with computer crimes, such as the manner and means of executing a search warrant on a computer center, pose unique problems which will have to be dealt with as they occur."

The most troublesome problems posed by computer fraud concern detection and proof, which are not cured by the proposed statute. Auditors find themselves stymied without carefully planned audit leads and program security. The new Federal Rules of Evidence recognize the necessity of establishing the standardization of the computer and the integrity of the data input before the printout will be accepted into evidence as an exception to the hearsay rule. Case law has been concerned with the "mystique" of the computer and its evidentiary output. See U.S. v. DeGeorgia, 420 F.2d 889 (9th Cir. 1969); U.S. v. Russo, 480 F.2d 1228 (6th Cir. 1973) cert. den. 414 U.S. 1157 (1973). Neither this proposed statute nor other proposals have been helpful in extending these limited aids to meet the technical and novel problems of procedure and proof in these computer fraud cases. (See also Tapper, Colin, "Evidence from Computers", 4 Rutgers Journal of Computers and the Law, 324 (1974), where the problem and statutory progress is discussed. See also Freed, Roy N., Computers and the Law, p. 46 et seq. (4th Ed.)).

Very little has been done to overcome obvious problems in discovery, search warrants, and subpoenas except for the impact of the Privacy Act. Further study must be undertaken to find solutions to the procedural and evidentiary problems that impede the detection and prosecution of computer crimes under existing law.

Respectfully submitted,

Tom Karas, Chairperson

April 3, 1979

Prepared Statement of Wayne Douglas Bennett

Sterling, Virginia
26 February 1980

Re: S.240, Federal Computer Systems Protection Act

Senator Orrin Hatch
Committee on the Judiciary
Russell Senate Office Building
Washington, D.C.

Dear Senator Hatch:

The revised S.240 (6 November 1979) is well drafted and seems to serve its purpose of facilitating prosecution of computer abuse. A significant problem remains, however, with respect to the word, "use."

"(U)se' includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer."

It seems clear from the definition of "use" that it does not include the notion, "cause to be used". Instruction, communication, data storage, data retrieval, logical use, arithmetic use, and memory usage are all more or less direct uses of computers. While this definition of "use" is simply intended to give examples (by the word "includes"), none of the examples connotes usage that is anything but direct. Thus submission of a batch job to an operator at a computer installation may not be use. Common sense indicates that the statute is intended to ensnare batch abusers as well as on-line abusers.

How far can this be taken? It seems, by virtue of the typesetter exclusion (from the definition of the word, "computer"), that causing an advertisement to be placed in a newspaper that employs automated typesetting cannot fall within the act, even if the advertisement is central to a scheme to defraud. On the other hand, it could be argued that the use of the computer was incidental to the fraud and that without the statutory exception, such perpetrators of fraud would fall within the scope of the act by virtue of the modernization of a particular newspaper's typesetting facility. This example is significant because it resembles a great many other situations wherein causing a computer to be used is simply an accident of the fraud. Thus, a credit card fraud will touch a computer installation as it unfolds. Is the fraudulent preparation of data that will ultimately be used as input to a computer program included within the scope of the act?

The question is really whether the "user", as defined by the act, must be the person who intends to defraud. Whenever the fraud requires the involvement of a computer in order for the fraud to be successful, "use" should be expanded to include "cause to be used." Conversely, whenever the involvement of a computer is a mere accident of the fraud, "use" should be construed in the more restricted sense (as currently defined in the bill). Indeed, the only awkwardly worded passage in the bill involves computer exclusions (typesetting devices and personal computers). It appears that the

real need for the typesetting exclusion arises because of the failure to adequately delimit the scope of the proscribed acts.

If the definition of the word "use" were expanded to include "intentionally cause to be used," indirect use of the computer would be included, but limited to cases where the computer is more or less essential to the scheme to defraud.

I applaud your attempt to facilitate the prosecution of computer crime and, as stated above, generally approve the statutory language. It is hoped that computer security practitioners (who have concentrated on prevention, not prosecution) will carefully note the provisions of S.240 and incorporate security measures which will aid in proof of computer abuse under the bill.

I appreciate the opportunity to present my opinion and request that this letter be included in the record of your hearings regarding the bill.

Respectfully,

Wayne Douglas Bennett

Wayne Douglas Bennett

36 Wedgedale Drive
Sterling, Virginia
22170

American Society for Industrial Security

25th year



2000 K Street, N.W., Suite 651 Washington, D.C. 20006 Telephone 202/331-7887

President

Albert S. Davis, CPP
Owens-Illinois Inc.
Toledo, Ohio

First Vice President

Louis A. Tyska, CPP
Timex Corporation
Waterbury, Connecticut

Second Vice President

Salvatore Gallo, CPP
Martin Marietta Corporation
Orlando, Florida

Third Vice President

Arthur A. Kingsbury, CPP
Macomb County Community College
Mount Clemens, Michigan

Secretary

Gerald S. Rees, CPP
Weyerhaeuser Company
Tacoma, Washington

Treasurer

John G. Wilkinson, CPP
Texaco Inc.
White Plains, New York

Chairman of the Board

Carl L. Carter, CPP
National Bank of Detroit
Detroit, Michigan

Other Directors

John V. Clark, CPP
The Boeing Company
Seattle, Washington

Robert H. Cobbs, CPP
Aeroyet Manufacturing Company
Fullerton, California

Clifford E. Evans, CPP
Digital Equipment Corporation
Phoenix, Arizona

Edward G. Goulart, CPP
MIT Lincoln Laboratory
Lexington, Massachusetts

Gordon W. Kettler, CPP
General Motors Corporation
Detroit, Michigan

Patricia C. Manion, CPP
Xerox Corporation
Stamford, Connecticut

Marilyn D. McNichol, CPP
Sierra Research Corporation
Buffalo, New York

Loren E. Newland, CPP
Ramada Inns
Phoenix, Arizona

Dennis A. Noggle, CPP
Kimberly-Clark Corporation
Neenah, Wisconsin

Alexander Smart, CPP
Royal Dutch Shell Group
London, England

John J. Thompson, CPP
Lockheed Georgia Company
Marietta, Georgia

Ralph O. Truet, CPP
AMTRAK
Washington, D.C.

Don W. Walker, CPP
GENESCO
Nashville, Tennessee

Raymond E. Williams, CPP
TRW Systems Group
San Bernardino, California

STATEMENT OF

THE AMERICAN SOCIETY FOR INDUSTRIAL SECURITY

CONCERNING THE

FEDERAL COMPUTER SYSTEMS PROTECTION ACT

OF 1979

(SENATE BILL S.240)

Mister Chairman and Members of the Judiciary Committee:

I am E. J. Criscuoli, Jr., Executive Director of the American Society for Industrial Security. On behalf of the officers, directors and members of the American Society for Industrial Security (ASIS) I take this opportunity to comment on the Federal Computer Systems Protection Act of 1979 (S.240). In commenting on this crucial piece of legislation, I draw on the expertise of many ASIS members and also on more than twenty-five years of personal experience at various levels in the field of security, in both the private and public sectors.

Computer crime is a growing and serious problem. Felons, armed with computer technology, presently bilk the public out of more than \$100 million annually; their ranks continue to grow. With the advent of the Electronic Funds Transfer Systems (EFTS), the present problem will soon be dwarfed. It is because of ASIS' concern with this area, that we strongly throw our support behind passage of Senate Bill S.240 by the U. S. Congress.

I. Concerns for the Problem of
Computer Crime

One of the fastest categories of crime is that in the computer area. With the proliferation of computer technology and also the advent of the Electronic Funds Transfer System (more than 1,200 banks have some form of rudimentary EFTS system at present), security and deterrence

have become serious problems. Computer crime is a challenge that afflicts both the private and governmental sectors. The following governmental officials have openly acknowledged the problems connected with computer crime (see Appendix A):

- the Office of Management and Budget
- the Department of Defense
- the Office of Inspector General, Department of Housing and Urban Development

Senator Ribicoff, as early as February 2, 1977, informed the U. S. Senate that:

"Today, for myself and Senator Charles H. Percy, the ranking minority member of the committee, I am announcing the issuance of a staff study entitled, 'Computer Security in Federal Programs.'

"The staff study demonstrates that the executive branch has neglected to take adequate steps to secure its computer systems. The staff study shows that computer security problems are especially prevalent in civilian agencies whose computer systems are involved in the disbursement of public funds, economically valuable data and privacy information."¹

A year later, on June 21, 1978, Senator Biden reiterated Senator Ribicoff's concerns and informed the U. S. Senate Subcommittee on Criminal Laws and Procedures that:

"The potential for abuse of the computer by criminals is as limitless as data processing technology itself. However, this crime of the future is already upon us."²

Senator Biden also went on to relate the ease with which computers are vulnerable to criminal attack:

"A student engineer in California developed a clever system, using the beeper tones from a telephone to gain access to the computer used by the Pacific Telephone & Telegraph Co. for controlling its equipment inventory. He used the computer to steal over \$1 million worth of equipment which he sold over a 3-year period before he was turned in by an associate."³

Senator Thurmond, also commenting on the problem has noted the following:

"The growth of computer technology in America has surpassed the ability of prosecution to prevent and prosecute computer-related crimes. White collar criminals have moved into the field because of the vulnerable aspects of computer operations. The sophisticated nature of a computer makes detection of criminal misuse most difficult and, once detected, makes investigation and prosecution equally hard."⁴

In recognition of the problems of computer fraud, and the need for adequate security in federal computer systems, the Office of Management and Budget (OMB) on July 27, 1978, issued Circular No. A-71. It calls for the establishment of management controls to safeguard personal, proprietary, and other sensitive data in federal computer systems; among them, the following:⁵

- establishing personnel security policies
- establishment of management controls
- assigning the responsibility for security to a management official within the agency
- establishment of policies and guidelines to ensure personnel and physical security of the system.

We at ASIS share the concern demonstrated by the above individuals, and organizations. There is sufficient justification to show concern in this area. We will in the pages that follow, address some of these concerns.

II. Dimensions of the Problem

The average computer crime is said to cost the public (business included) in excess of \$400,000.⁶ The Chamber of Commerce of the United States places at the annual cost in excess of \$100 million (see Appendix B). Further, the computer easily lends itself to be employed (in a

secondary role) in other white collar frauds. We at ASIS are extremely concerned that we may be witnessing only the tip of the iceberg.⁷

Computers are vulnerable to attack from four areas: external physical attacks (destruction of all or part of a facility); internal physical attacks (sabotage); internal manipulation of the data (input) and instructions (programs); and electronic penetration of the system.

External physical attacks may come from: the lone criminal (the mentally unstable, or disgruntled employee, or even an extortionist); terrorist group(s); or organized crime types (for purposes of extortion, collusion with management in a scheme to defraud the insurer, or in an effort to neutralize a competitor). External physical attacks can take the form of destruction directed at the computer facility itself, parts of its components, or at the communication phase.

Internal physical attacks can come from several sources: a disgruntled or mentally unbalanced employee ("get even with employer"); an agent(s) of a terrorist group (motivated by ideology, personal feelings for a member of the terrorist group, blackmail, threats against his life or that of his family, or financial gain); industrial or foreign spies or their agents (in an attempt to neutralize a facility for economic or political gain); and organized crime or their agents (extortion, in the pay of others, part of a larger conspiracy to defraud, or related to labor-management disputes).

Internal physical attacks can be directed at one or more of the various phases of a computer operation. They can be directed at the input phase of the system; the system's capability to translate data into signals for purposes of computation or transmission is destroyed. It can also take the form of the destruction of the system's software; or the

destruction of the system's output capability. Attacks can also be directed at the Central Processing Unit; thus, preventing the system from retrieving data stored in its files.

Of equal concern is the threat of the internal manipulation of computer systems. Input data can be manipulated: altered, fabricated, or destroyed. In addition, the software (programs employed to run these systems) can likewise be manipulated to fit the needs of the felon(s). Output data can also be tampered with: modified, fabricated, or destroyed.

Also of concern in a computer environment is the threat of electronic penetration of the system. Especially vulnerable to attack is the communication phase of the system. This phase involves the transmission of data back and forth between: terminals, computers, and terminals and computers. The threat at this stage comes from felons armed with electronic interception tools. Electronic entry tools require a degree of sophistication and technical know-how that is not readily available to lone criminals. Members of organized crime (or their associates), terrorist groups, espionage networks, and white collar criminal rings have both access to these systems, and the technical know-how to penetrate them.

Electronic interceptive tools are presently readily available. Sophisticated criminals, with the necessary technical know-how, can easily employ these tools of modern technology against a computer system. Data communications can be intercepted, recorded and modified. The threat from organized crime and espionage networks is paramount in this area. Terrorist groups and white collar criminal rings should also not be dismissed. The threat from the lone criminal in this area is of lesser concern. To highlight our concern, we quote from the testimony of one Bobbie Miller, an alleged former member of organized crime:

"Q. Did you fear detection by the police?

A. No, sir.

Q. Why not?

A. Like I said, we just had more sophisticated equipment than them, you know. When you see what somebody else is doing, it's not hard to leave before they get there.

Q. How would you know, sir, what the police were doing?

A. Monitoring them 24 hours a day.

Q. How?

A. Well, we had pretty elaborate radio systems for the organized crime units, detective units and broke down their codes.

Q. You're saying then that you monitored the police or the law enforcement frequencies?

A. Yes, sir.

Q. And tried to break down their codes?

A. Didn't try, broke their codes.

Q. You broke them?

A. Yes, sir." ⁸

III. Portrait of a Computer Felon

The electronic felon is often portrayed as being young, adventure-some, intelligent, arrogant, and as one who perceives himself to be a modern "Robin Hood", striking back at modern technology.⁹ We are also told that this new breed of criminal is drawn to computer related crimes because of the challenge that modern technology poses. The felon is portrayed as viewing crime as one giant game: monetary gain, we are told, comes to play a secondary role.¹⁰ The profile that has emerged in the last several years can often be misleading, and can undermine efforts to address computer crime.

The picture of the lone felon; armed with the knowledge of modern science, and motivated by the challenge of beating the system dismisses reality. The lone felon poses a secondary threat to a computer system. The serious threat comes from the professional criminal. It can safely be said that adequate physical and personnel security measures could be enacted to curtail somewhat the activities of the lone criminal. In addition, the losses a lone felon can inflict on a computer system can be minimized and contained by our present technology.

The serious threat to computers comes from professional white collar criminal groups. Studies of securities frauds, scams, insurance frauds, and an array of consumer related frauds, indicate that there are numerous groups with criminal inclinations, that specialize in white collar crimes. These criminal groups come from diverse social and economic backgrounds, depending upon their specialization. However, a well organized conspiracy involving organized white collar felons can pose a serious threat to a computer system. Well organized and funded; technically capable, and with access to key personnel in the financial arena, these white collar felon rings can easily attack computers.

Organized crime is also cause for serious concern. This confederation of well organized professional criminals has increasingly grown in sophistication, and has made inroads into the computer area.¹¹ Computers offer these organized criminal groups diverse and varied opportunities. Given their structure, contacts, and ability to coerce and win over employees at computer facilities, organized crime poses a serious threat. The Syndicate brings with it not only its contacts, know-how, and organization, but also both national and international fencing operations. Further, loansharking, bookmaking and narcotics provide a ready-made tool to penetrate and subvert employees of a computer operation. Of special concern

to us, as regards organized crime, is the testimony of James York, Chief of Police for Orlando, Florida:

"An organized crime activity of significant import in the Orlando area is marketing of stolen goods. Several recent investigations in our area indicate an alarming amount of stolen goods being moved through retail outlets such as second-hand stores and so-called flea markets. These outlets for stolen goods are indispensable to burglars and thieves and serve as primary motivation for related crime."¹²

Another threat to computers (often neglected), comes from the growing problem of domestic and international terrorism. Professional terrorist groups are presently active in dozens of countries. Terrorists have also struck targets within this country. The terrorist, unlike the criminal, is motivated by ideological fervor. Monetary objectives play only a secondary role in the terrorist's activities; what makes the terrorist potentially dangerous is his willingness to sacrifice both himself and others for his cause. Computer systems increasingly attract the attention of terrorists.¹³

IV. Need for Security

The problem of computer crime is a complex one. S.240 alone will not suffice to deter crimes by computer felons. There is need for security. Numerous security measures (physical and personnel) have been recommended for safeguarding computers. Senator Ribicoff has pointed out, that his staff has found in its study of federal computer programs that good security measures can plan a role in safeguarding these systems from both internal and external criminal attacks. There is little or no dispute that there is a need for security both in the

private and public sectors. However, two questions are often raised:

- how much security?
- and at what cost?

Unfortunately these two questions remain as yet to be answered.

Security can be divided into two key components: physical and personnel. Physical security is connected largely with the construction, location, storage and entrances of a computer operation. It encompasses the hardware and software of the system; as well as the connecting terminals, and lines employed by a computer to transmit the data. In an era of growing terrorism, physical security has increasingly come to play an important role.

However, although there is a consensus that physical security can play a role in safeguarding computer systems, both the private and public sectors have shown laxity in enacting needed physical security measures. In part, both labor unions and consumer advocates have shown, traditionally, opposition to such measures. Society has shown a reluctance to swallow the "physical security pill". However, physical security must be brought to bear if we are to curtail computer crime.

Personnel security, often neglected, is also of paramount importance in any meaningful computer security program. Physical security often deters the unsophisticated external criminal. However, the sophisticated felon, and the disgruntled employee, often, must be deterred by personnel security. It is breaches in personnel security that pose a serious threat for computer operations. Breaches in personnel security have often enabled professional criminals and terrorists to penetrate computer systems. Our experience with computer crime should be sufficient indicia

of potential problems employee security breaches can cause for computer operations. Presently, however, personnel security programs find themselves hampered by an array of legislation that makes it often impossible to screen felons.

V. Advent of EFTS and EMS

We are presently witnessing an electronic-informational revolution in this country. The Electronic Funds Transfer System (EFTS), and the Electronic Mail System (EMS) have made their entry. EFTS has taken root; EMS will soon do so, and both raise with them the spectre of additional computer related crimes. S.240 should, unless emasculated, assist law enforcement in combating EFTS and EMS crimes.

A. EFTS

The Electronic Funds Transfer System can best be described as a growing array of financial services; among the ones most frequently identified with it are: wire transfer of funds; direct deposit of income checks; periodic or authorized payments; credit card authorizations; check verification; point-of-sale payments (POS); cash dispensing machines (ATMs); automated clearing house facilities (ACHs); as well as data capture, analysis, and billing systems (example, electronic cash registers that record data to monitor inventory quantities and aid management in pricing and other decisions). Numerous definitions have been put forth to define EFTS. It has been defined as payment systems that use computerized electronic impulses rather than paper - (money, checks, etc.) - to effect an economic exchange.¹⁴ EFTS has also been defined as a class of related practices and technologies; which uses electronic impulses,

generated and interpreted by computers, to debit and credit financial accounts. Each such debit or credit transaction is termed an electronic funds transfer.¹⁵

EFTS represents a medium for the transfer of funds, through the use of electronic impulses. The systems take on numerous forms, and rely on the computer as their everyday workhorse. These systems have the potential to operate regionally, nationally, or even internationally. Proponents view EFTS as a superior way to communicate and transport data, consolidate information, and provide customers with direct and discretionary access to financial transactions and records. EFTS, however, will also find itself the target of an array of criminal and terrorist groups. We must take steps now to safeguard it.

B. EMS

The Electronic Mail System can be defined as data transmission systems, that use electronic impulses rather than paper, to effect the flow of information. These systems have come to embrace a wide range of services; among them, the: Electronic Computer Originated Mail (ECOM), Electronic Message Services (EMSS), Intelpost, and the Society for World-wide Interbank Financial Telecommunications (SWIFT).¹⁶ Proponents view these systems as replacements for the present postal, telex, and cable communicating systems.

ECOM is an experimental mailgram-type service; it would be limited to mass mailers, who send a minimum of 5,000 messages a month. ECOM would be run by the U. S. Postal Service (USPS), and would link the nation's 25 largest post offices.¹⁷ In an ECOM system, messages are recorded initially on magnetic tape or disc by the user, and are then transmitted, on-line, from the user's premises to each destination post office. Upon destination, the messages are then converted into hard copy and delivered to the

recipient by a mail carrier. Deliveries would be made within a day from the input time. ECOM would also offer a variety of address and text editing features. Deliveries would be made within a day from the input time. Deliveries of the same message could be made to multiple addresses; portions or even the entire message sent to a specified addressee, could be altered.

Another EMS system currently being developed by the USPS is Intelpost; it is currently undergoing a one-year field test. Similar to ECOM in its workings, it would provide service between this country and several other European nations. There are an array of other experimental EMS systems. Western Union is testing an International Mailgram Service (IMS); the Xerox Corporation is experimenting with the Telecommunications Network Service (TNS), and USPS has demonstrated an eagerness to compete with its MAILGRAM. In the not distant future, customers with the needed computer capability will be able to send messages electronically through EMS. Like EFTS, EMS may also find itself the target of criminals.

Conclusion

We, at ASIS, have shown a concern in S.240 from its inception. When first introduced, we took the position that we need strong legislation in this area. As technology advances, the fabric of the law must keep pace with it. The Society is prepared to assist this Committee in any way it can; we have the experts and the will to come forth and offer our expertise and experience in this area. Our Computer Security Committee and its Chairman have been of great assistance to this Committee's staff in the past, and have indicated a willingness to continue to assist.

In closing, I would like to note that ASIS is grateful to have been afforded this additional opportunity to comment on S.240. We strongly urge that S.240 become a reality.

Sources

- ¹ Congressional Record, Vol. 123, No. 19, February 2, 1977, p. 1.
- ² Senate Subcommittee on Criminal Laws and Procedures, Hearings on the Federal Computer Systems Protection Act (Washington, D.C.: U. S. Government Printing Office, 1979), pp. 1-2.
- ³ Ibid., p. 2.
- ⁴ Ibid., pp. 5-6.
- ⁵ See OMB Circular A-71 and Transmittal Memorandum No. 1, of July 27, 1978, for added details.
- ⁶ Brandt Allen, "The Biggest Computer Frauds: Lessons for CPAs," Journal of Accounting, May 1977, p. 53.
- ⁷ August Bequai, Computer Crime (Lexington, Mass.: D. C. Heath, 1978), pp. 181-195; also see Bequai, White Collar Crime: A Twentieth Century Crisis (D. C. Heath, 1978), pp. 163-170.
- ⁸ Florida House of Representatives Select Committee on Organized Crime, Final Report on Organized Crime for 1978, (Tallahassee, Florida: State Capital, 1979), p. 34.
- ⁹ Tim A. Shabeck, Computer Crime (Madison, Wisconsin: Assets Protection, 1979), pp. 4-6.
- ¹⁰ Ibid., p. 6.
- ¹¹ August Bequai, Organized Crime (Lexington, Mass.: D. C. Heath & Co., 1979), pp. 183-191.
- ¹² Florida Select Committee on Organized Crime, Final Report on Organized Crime, p. 56.
- ¹³ Computer attacks by terrorists have been reported in Europe, Asia, Africa, and Latin America.
- ¹⁴ Carol A. Schaller, "The Evolution of EFTS," Journal of Accountancy, October 1978, p. 78.
- ¹⁵ Mary G. Bender, Electronic Funds Transfer Systems (New York: Kennikut Press, 1975), p. 37.
- ¹⁶ Phil Hirsch, "FCC Eyes Xten as Revolutionary," Computerworld, September 17, 1979, p. 2.
- ¹⁷ Presently the Postal Service and the FCC are involved in a jurisdictional dispute over EMS.

Prepared Statement of



February 26, 1980

The Honorable Paul Laxalt
United States Senate
Washington, D.C. 20510

Dear Senator Laxalt:

It is a pleasure to respond to the request from your legislative counsel, Mr. Jock Nash, for comments on S-240 and its House companion H.R. 6192. For the record I commented on a prior bill, S-1766, and my remarks appear on page 135 of the Hearings held by the Senate Subcommittee on Criminal Law and Procedures, June 21-22, 1978.

While H.R. 6192--and I presume that S-240 has been amended to agree with it--is a vast improvement over earlier efforts, I still find it to be unsatisfactory legislation. I am afraid that the Congress of the United States has not heeded the words of the Lord High Executioner and made "the punishment fit the crime." As presently worded, the bill continues to make a federal offense of many computer-related activities that are not worthy of legal attention. Rather, they are either trivial activities; or have consequences best described as nuisances. Such lesser infractions are properly dealt with through management discipline, employee termination, suspension of pay, or whatever--but certainly not by federal criminal action with possibly large penalties.

Of all the things that can be done and are done by a computer, H.R. 6192 does not properly distinguish the ones which are of sufficient serious social or criminal consequence and therefore need legal attention. In this regard, I call your attention to Florida House Bill No. 1305 that was introduced in 1978. While I would not assert that the structure of the Florida bill is precisely what might be needed at the federal level, it is nonetheless a better model of what needs to be done. The Florida legislation at least makes an effort to identify various kinds of criminal acts relevant to computers, and adjusts the penalties and legal consequences appropriately.

In preparation for preparing these comments, I have read an article "On Computer Crime--Senate Bill S-240" by John K. Taber on pp. 517ff of the Computer Law Journal. Some of his criticisms have been accommodated in the wording of H.R. 6192, but there are a substantial number of his comments that continue to be true for it. I subscribe to his views and would add my comments as follows.

A computer has always been associated with mystique; partly for that reason, a rather extensive lore of mythology has accumulated around it. While I would not deny for a moment that there surely have been criminal acts in which a computer played some role, I would ask whether the evidence justifies the view that a computer is so significantly different that a special law is needed. Or is it more mythology? As Taber elaborately documents, the well-known studies of Parker and Nycum at SRI do not support the assertion that computer-related crime is a matter of great social consequence.

I would note that in many aspects of computer affairs, individuals--especially managers--and institutions create enormous difficulties for themselves by believing that a computer system is mysteriously different; and therefore cannot be dealt with by well-established and accepted mechanisms. For those criminal activities in which a computer might be a part, should we think of a computer like a gun, which obviously can inflict great bodily harm to a human body; or should we think of it as a file cabinet--a repository of information that can be used for various criminal or socially undesirable acts? If the latter is the right analogy, then why should physical damage to a computer be a federal offense when prying open a file cabinet is not? One might also try the analogy that a computer is like a bank vault in that the contents of either have great monetary value. If that is the appropriate analogy, then I note that there is no law against damaging a vault; the crime is theft of its contents.

To illustrate a loophole in the present bill, let us suppose that with my personal household computer I devise a fraudulent scheme that I carry out with the aid of my computer and that I do so with interstate consequences against a financial institution. As "computer" is now defined in H.R. 1692, I would escape its consequences. Now suppose that I plan the fraud with computer time that I legitimately purchase on a computer owned by a defense contractor but I execute the fraud with my household computer. Am I subject to H.R. 1692 or not? Finally, I plan the fraud by bootlegging time on a federally owned computer but I execute with my household computer; what now is the situation? Also please note that in all the above scenarios, my "household computer" could be a hand-held calculator!

I suggest such twists and turns to illustrate what I believe to be true. While the Parker-Nycum work has demonstrated the existence of criminal activities in which a computer plays a role, the dimensions of the matter have not been carefully thought through nor the issue adequately structured. Some of the presumably undesirable things that can be done with a computer are employee infractions; others are nuisances; others are trivial capers by ingenious computer users; some perpetrate a fraud

against a large number of individuals; some permit embezzlement; and in principle, at least, an occasional one could lead to widespread havoc of some kind. It simply is inappropriate to consider such a broad spectrum of activities as a uniform federal offense requiring vigorous legal action.

To illustrate what I think needs to be done, let me cite a case that the press reported recently describing the use of computers at the Social Security Administration to usurp funds for personal gain. If the participants in this crime had perpetrated their act by stealing money from a locked file cabinet, the crime would be that of theft. Under H.R. 6192 however, since the crime was committed with the aid of a computer, it would have a special status and the legal penalties for the perpetrators correspondingly different. It seems unwise to create such anomalies of law.

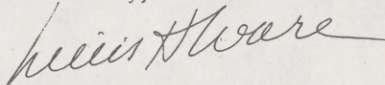
There is no question but that a computer or a computer system can be the instrumentality by which a criminal act is committed, but we must decide whether this single fact is sufficient reason for special legislation. I appreciate that robbery and armed robbery are treated differently under the law, presumably because the use of firearms signifies more malicious intent on the part of the criminal or perhaps because the victim is at more risk. Should a corresponding argument be applied to computers; and if so, what is the evidence that might support such a view? In what way does a computer permit one or more individuals to perpetrate criminal acts that are in some way more heinous, more devastating to society, different, more evil, less socially desirable... than similar criminal acts undertaken by more usual methods.

As you can tell from my line of reasoning, I believe that we do not yet have a satisfactory intellectual understanding of the criminal behavior that is in some way related to computers. I therefore believe that we are not yet ready to pass legislative controls. Until Congress can satisfactorily answer questions such as I have raised, my guidance would be: "Back to the drawing board because we have not yet properly understood the intricacies and dimensions of a very complex question; neither have we yet correctly identified the proper way to perceive a computer in its role as a possible instrumentality of criminal acts." At this point in time my view is that H.R. 6192 and S-240 (as amended) are best left without further action until more very essential homework gets done.

My intuition is that when we do understand the problem with insight and perspective, a law structured quite differently will be required.

Whether S-240 and H.R. 6192 could be satisfactorily amended or would have to be scrapped remains to be seen.

Sincerely,



Willis H. Ware
Corporate Research Staff



Prepared Statement of
Association for Computing Machinery

1133 AVENUE OF THE AMERICAS
NEW YORK, NY 10036
(212) 265-6300

DANIEL D. McCracken
President

Reply To: 7 Sherwood Avenue
Ossining, NY 10562
914 941-2100

March 5, 1979

Senator Abraham A. Ribicoff
United States Senate
Washington, DC 20510

Dear Senator Ribicoff:

I write to add my support to the positions expressed by Mr. Donn B. Parker on S240 as stated in his letter to Mr. Mark Gittenstein.

Mr. Parker, as you know, is without any doubt the country's most senior and most respected expert on computer-related crime, through his NSF-sponsored workshop, his research, his wide speaking, and through his influential book on the subject. His opinions, which have been supported by other senior people in the Association for Computing Machinery, including several with competence in both computing and the law, deserve most careful attention.

My own involvement is less direct, but in the more restricted concerns of EFT and the NCIC, not entirely through the Association, I am also on record in support of responsible legislation, and have previously written you to that effect.

If there is any way our organization, the largest and oldest in the field, can be of any assistance to you, we would be glad to do so.

Sincerely yours,

Daniel D. McCracken

DDM:ter

cc: Donn E. Parker
Mark Gittenstein
Sidney Weinstein, ACM Executive Director
John Tartar, ACM External Activities Board Chairman
Susan Nycum, Esq., ACM Legal Issues in Computing Chairman
Peter Denning, ACM Vice President

Prepared Statement of
THE GREENWICH SAVINGS BANK

BROADWAY AND SIXTH AVENUE
AT THIRTY-SIXTH STREET
NEW YORK, N. Y. 10018

DANIEL STACK
SENIOR VICE PRESIDENT AND COUNSEL
(212) 868-8907

February 2, 1979

Senator Joseph Biden
Chairman, Subcommittee on Criminal Laws and Procedures
Senate Office Building
Washington, D. C. 20510

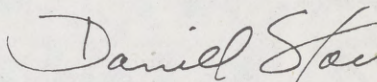
Dear Senator Biden:

I would like to take this opportunity to express my wholehearted support for the efforts which you and your colleagues are making to pass Senate Bill 240 dealing with fraudulent and illegal uses of computer systems.

The growth of computers in importance in every aspect of American life mandates that proper protective laws be enacted so that the American public and its institutions can enjoy the fruits of American technical innovation without fear of loss of assets or privacy.

Again, we applaud you for your far-sighted efforts in this most important field.

Very respectfully,


Daniel Stack

DS:JB

cc: Senator Abraham Ribicoff

Prepared Statement of
NATIONWIDE FINANCIAL SERVICES CORPORATION

A SUBSIDIARY OF
CITICORP



January 5, 1979

Senator J. R. Biden, Jr.
Subcommittee on Criminal Law and Procedures
Room 2204, Dirksen Office Building
Washington, D.C. 20510

Dear Senator Biden:

I have read with interest the proposed amendment to Chapter 47 of Title 18, United States Code. The need for this Federal Computer System Protection Act is obvious and an "idea whose time has come". As an EDP Inspection Manager for the Citicorp subsidiary Nationwide Financial Services Corporation and a former Special Agent, Computer Security Division, U.S. Army Intelligence Agency, I have been intimately involved with computer security requirements of both a financial concern and a Federal agency handling compartmented classified information.

I am concerned with both the language and definitions contained within this proposed legislation, specifically subparagraph (b), which states:

"(b) Whoever, intentionally and without authorization, directly or indirectly accesses, alters, damages, or destroys any computer, or any computer software, program or data contained in such computer, computer system, or computer network, shall be fined not more than \$50,000, or imprisoned not more than 15 years, or both."

This paragraph completely ignores malicious intent of commission. By strict application of this above statement, most of the persons I know who are involved in computer security related professions would become unindicted felons. Another point within this subparagraph is the proviso concerning "computer software, program, or data contained in such computer". It should be emphasized that alteration can occur outside the computer (i.e., if alterations to off-line source code were undetected, these alterations could become part of the executable module if recompilation of this source were required).

Concerning subparagraph (c), the definition of terms used in (a) and (b); I am sure more competent persons than myself have commented on these definitions. Suffice it to say that I do not believe these to have been written by someone having sound data processing experience. For example, "access" meaning to "approach" a computer. How do you approach a computer? I'm sure our computer would like

to be approached from the west by console operators on their knees, bowing and genuflecting, praying for millisecond response time to our terminal session users. A law concerning this concept of "approaching a computer" appears to bear serious implications toward freedom of religion for computer aficionados.

From this reading of the proposed law, I turned to Senator Ribicoff's statements concerning the bill as reported in his testimony to the Criminal Laws and Procedures Subcommittee of the Senate Judiciary Committee and the June 27, 1977 Senate Congressional Record. In this explanation, Senator Ribicoff further defines "access" to a computer. One item he uses as an example, radiation, causes concern. Radiation is defined in both references as passive eavesdropping without direct connection via detection of acoustical or electromagnetic signals emanating from a computer. This is the area known in the profession as TEMPEST. As far as I know, all TEMPEST principles and specifications are classified in the interest of national security. It does little good to define a bill in terms that are not accessible to the public. Further, all four "penetrations" given as criminal access are external to the system. This ignores one of the basic findings of computer crime analysis -- the penetrator was usually an insider (or has extensive inside collusion). Of course, there are exceptions such as the well-publicized Jerry Schneider incident. However, most studies (notable ones include SRI's Donn Parker's "Computer Abuse" and University of Virginia's Brandt Allen's "The Biggest Computer Frauds") emphasize that less than 10% of all known computer frauds were perpetrated solely by outsiders to the organization.

Concerning Senator Ribicoff's definitions of what this bill will make illegal, I feel he has dealt with a glamorous TV wiretapping scenario. A better example would be the following:

1. Unauthorized disclosure of information.
2. Unauthorized access to information.
3. Unauthorized modification to information.
4. Unauthorized denial of service.

Broadly speaking, this would cover all aspects of computer crime if information includes that needed documentation to run a system, all automated files and programs, and all automated listings (including computer printed negotiable items). It would also cover the unauthorized giving and receiving of such information.

Finally, a bill such as this can be a milestone in protecting against spreading computer crime. However, an item of this importance should be defined exactly as to its intent and provisions.

Respectfully yours,


Gary Mevius,
EDP Inspection Manager

Prepared Statement of



ELECTRONIC FUNDS TRANSFER ASSOCIATION

Suite 502, 1029 Vermont Avenue, N.W., Washington, D.C. 20005 202/783-3555

February 7, 1979

CHAIRMAN OF THE BOARD

Roland R. Eppley, Jr.
Eastern States Bancard
Association, Inc.

EXECUTIVE COMMITTEE

M. M. Alafia
Atalla Technologies
Robert F. Barone
Diebold Incorporated
Lawrence A. Ladouceur
The Greenwich Savings Bank
Howard Mandelbaum
Manufacturers Hanover
Trust Company
John J. McDonnell, Jr.
TYMENET
William H. Robinson, Sr.
Wilmington Savings
Fund Society
Samuel F. Shewhan
General Telephone and
Electronics

BOARD OF GOVERNORS MEMBERS

Charles F. Anderson
Northwest Management
Services, Inc.
Liam Carmody
First National State Bank
of New Jersey
Robert A. Chapman
System Development Corporation
William Carrington
Financial Data Systems, Inc.
Gary E. Daniel
Burroughs Corporation
Timothy M. Hammonds
Food Marketing Institute
Paul L. Heifer
Western Bancorporation
James T. Kinsey
Signal Financial Corporation
Lawrence F. Linden
Malco Plastics, Inc.
Patrick S. Portway
Satellite Business Systems
William C. Walker
GE Credit Corporation

OFFICERS

Henry v. Z. Hyde, Jr.
President
Roger V. Barff, Esquire
General Counsel/Secretary
Howard G. Johnson
Treasurer
Price Waterhouse and Co.

The Honorable Joseph R. Biden
United States Senate
Washington, DC 20510

Dear Senator Biden:

Because the Federal Computer Systems Protection Act (S. 240) has been assigned to your Subcommittee on Criminal Laws and Procedures, the Electronic Funds Transfer Association is most pleased to submit consensus recommendations of our special forum on the bill held January 29.

Support for this bill was substantial. The proposal is clearly the proper legislative remedy for computer crime. Consensus recommendations of the forum are attached.

Two problems remain: determination of whether or not access was "authorized" and evidence necessary for successful prosecution. In part, the question of authorized access can be answered by addition of a purpose clause and in part, depend on policy and practice of the computer owner. We support this approach.

The evidence problem is most difficult and expected to be worked out on a case by case basis. The Electronic Funds Transfer Association is available to you and your staff to do anything we can on this problem including additional discussions and recommendations if you wish.

We take special note of the excellent work of Mark Gittenstein, Chief Counsel of the Subcommittee on Criminal Laws and Procedures and Philip Manuel, Investigator, Subcommittee on Permanent Investigations. They have done an exceptional job and their knowledge and leadership is admired by the EFT industry.

Cordially,

Henry v. Z. Hyde, Jr.
President

Enclosure

ELECTRONIC FUNDS
TRANSFER ASSOCIATION

CONSENSUS RECOMMENDATIONS BY THE
FEDERAL COMPUTER SYSTEMS PROTECTION ACT FORUM

sponsored
by

The Electronic Funds Transfer Association
January 29, 1979 Washington, DC

The following recommendations represent the consensus of the conference with regard to the Federal Computer Systems Protection Act of 1979, introduced on January 25 by Senator Ribicoff and others.

Section 1028 (b) Computer Fraud and Abuse

Two elements should be added: (1) A purpose clause to make it clear that access must be for wrongful purposes; and (2) a provision covering authorized accessing for those wrongful purposes.

Addition of a purpose clause would add a necessary clarification of wrongdoing which is normally for either personal gain or destruction. For example, as written it would make it difficult to dispose of a used computer without clear and specific written authorization. Also, an innocent, inadvertent trespass could subject a person to severe liability. The purpose clause must include the concepts of trespass and willful damage.

Penalties may be too severe. A misdemeanor penalty and civil recovery should be added with fines going to the injured party up to extent of loss.

The severe level of penalties in the proposed bill may actually dissuade reporting of wrongdoing. Scaling the criminal penalty should overcome such resistance. In addition, if fines and money damages were made available to the injured party, reporting would be encouraged.

Include third party wrongful beneficiary. It should be made clear a third party can be a part of the wrongful activity and/or beneficiary of it even though there was no actual activity on the part of that person.

The word 'alters' in the second line of Section 1028 (b) is ambiguous. The words 'change' or 'modify' are preferable.

There are cases where university students have actually changed their academic record and situations in corporations where there have been additions or deletions to programs and records. While these are clearly alterations, they are more accurately described as 'changes' and 'modifications'.

Section 1028 (c) Definitions

"COMPUTER" The word 'electronic' in the first line of definitional terms 'electronic device' should be eliminated. The function of the word is not clear, adds nothing to the definition, limits the scope of the Act and

may raise an unintended defense.

"COMPUTER NETWORK" The intent of the Act appears to be expansion on the definition of 'computer system' by adding the concept of communications systems and/or combination of communications.

This sequence of definitions needs to reflect four elements with combinations: Computer; computer and software; computer, software and terminal; computer, software, terminal(s), and combination of communications systems. The word 'interconnection' could also be too limiting if it means physical connection. It is entirely possible to communicate by radio which may be improperly excluded by the word 'interconnection' if it means physical connection by telephone lines. The concept that needs to be in this definition is interfacing of any set of related computers via some form of communications systems.

The following definition of 'computer network' would contemplate these concepts:
" 'Computer Network' means the interconnection of any set of computers and terminals through a communications network. "

"COMPUTER PROGRAM" The word 'results' should replace 'products' appearing in the last line. While a computer may have products in the form of a printed report, 'results' is a broader concept more appropriate to computer use.

Prepared Statement of SRI International



December 20, 1979

Ms. Kathy Zebrowski
U.S. Senate
Subcommittee on Criminal Justice
Washington, D.C. 20510

Dear Kathy:

Here are my comments and concerns as you requested on S240 as reported out of the U.S. Senate Subcommittee on Criminal Justice on November 6, 1979. These comments are based on my 30 years of experience in research, programming, operating and managing computers and for the past 9 years doing research on computer abuse as a National Science Foundation grantee at SRI International.

The exclusions in the definition of a computer, part (c) are not effective, correct or practical and should be stricken. The text of concern is: "...but does not include an automated typewriter or typesetter, or any computer designed and manufactured for and which is used exclusively for routine personal, family, or household purposes including a portable hand-held electronic calculator".

The terms "automated typewriter or typesetter" and "portable hand-held electronic calculator" are not precisely defined, have many changing meanings and include many computers for which the bill was originally meant to and should include. Don't try to exclude devices when the real purpose may be to exclude certain uses. Devices change rapidly as technology advances. Whatever an automated typewriter is today will be different tomorrow. Today it could mean a typewriter with ribbon cartridge, automatic erasure, interconnection to a computer (a computer terminal) or a computer output printer incapable of use as an input device or as a typewriter. Tomorrow it could mean a voice-actuated typewriter.

Concerning calculators, the adjectives "portable" and "hand-held" are redundant. In addition, a calculator today can be programmable and be as powerful as a minicomputer with limited storage. Tomorrow it could be equivalent to some of the largest computers in use today and be able to store millions and billions of bits of data. Don't try to exclude them.

The exclusion of "...any computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes..." might be a reasonable exclusion under "use" with one exception. The word "routine" is not appropriate, because its use means that new or innovative non-routine personal, family or household purposes would not be excluded and should be. Therefore, maintenance of a Christmas card mailing list would be excluded but

SRI International

333 Ravenswood Ave. • Menlo Park, CA 94025 • (415) 326-6200 • Cable: SRI INTL MNP • TWX: 910-373-1246

how routine would a new mathematical method of calculating female menstrual periods be? That would probably not be routine at first but after coming into common use, it would become routine.

Don't exclude devices; only exclude uses if necessary. Leave it to the courts to decide what is a computer and a significant violation within the technology of the times. If the intent is to exclude letter, report, literary, news or educational writing by computer, then exclude those uses under the "use" definition but don't try to exclude devices or uses that could also be involved in heinous crimes.

Other, more minor definition problems should also be corrected. The phrase, "... by electronic manipulation" in defining a computer technologically is ambiguous and dated. Future computers may not be electronic, and manipulation may not adequately describe the functioning of electronic circuits and execution of compute programs. The definition is adequate without this phrase. Finally, in the definition of "use" use "storage functions", not "memory functions" to be consistent with the rest of the text.

I hope that these ideas will be helpful to you and lead to a stronger and better bill.

Very truly yours,

Donn B Parker

Donn B. Parker
Senior Managements Systems Consultant
Computer Security Program

DBP:lb
Encl.

cc: S. Nycum
J. Fugals
K. Curtis

Prepared Statement of H. Stuart Knight

On behalf of the Secret Service I would like to take this opportunity to comment on the Federal Computer Systems Protection Act of 1979 (S.240) and the role of the Secret Service regarding this bill. The Secret Service has spent more than two years in the research and preparation of programs to meet the challenges of computer crime. This statement reflects the Secret Service's long standing interest in this area.

Computer related crime is a growing and serious problem for the federal government as criminals are presently stealing with impunity millions of dollars annually. The Secret Service takes a serious view of the problem, and hopes to increasingly play a deterrent role in this area. S. 240 can prove to be a valuable medium for the Service which has both the requisite will and training to employ if Congress so provides.

The investigative responsibilities of the U.S. Secret Service are defined in Section 3056, title 18, United States Code. These responsibilities include detecting and arresting persons committing any offense against the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; and detecting and arresting persons violating certain laws relating to the Federal Deposit Insurance Corporation, Federal land banks, jointstock land banks, and Federal land bank associations.

For the past 114 years, the Secret Service has been the guardian of our nation's currency and has maintained the integrity of the federal payment system which issues government financial instruments such as U.S. Treasury checks, bonds, and securities by enforcing the laws relating to counterfeit and forgery.

However, in the near future, we may live in a world where paper money is a rarity. The Bureau of Government Financial Operations, Fiscal Service, Department of Treasury, in its January, 1980 statistical summary of the Direct Deposit Program, indicates that approximately 26% of the federal payment system is now electronically transferred and directly deposited. Projections made by Treasury officials estimate that by 1985 approximately 80% of the federal payment system will be processed electronically. The current monthly percentage represents over 11 million transactions involving five billion dollars in government funds. It becomes clear that while the Secret Service continues to investigate crimes historically within our purview, this agency can expect to find itself involved in a significant number of computer related cases.

The Treasury Department's direct deposit system of payments to check recipients represents only the beginning of a national electronic fund transfer system. Currency, and stock certificates will take on a less significant role in our financial market places. The Secret Service has already observed a shifting pattern of criminal activity in forgery related investigations. Our agency is uncovering individuals who are forging stolen government checks and using the proceeds to open an account in the payees' name. Simultaneously, the forger executes a request for direct deposit of future benefits. Consequently, the proceeds for that payee are electronically deposited to the fictitious account for ready withdrawal by the forger. What initially was a routine check forgery has now expanded into a computer related crime.

In the area of direct fraudulent computer manipulation, the Secret Service has successfully investigated and prosecuted these activities utilizing our current jurisdictional authority. One such investigation by Agents of this Service has resulted in the recent indictment of an employee of the Social Security Administration who allegedly manipulated a computer at a disbursement center in order to pay herself and two accomplices more than \$500,000 in monthly disability benefit checks. The same computer sends out 1.1 billion dollars in disability checks to 4.8 million workers and their dependents each month.

Another case which the Secret Service recently investigated involved a civilian pay clerk for the District of Columbia who developed a scheme to manipulate a computer which resulted in the fraudulent issuance of \$45,000 in checks to non-deserving recipients. The suspects involved were charged with forgery, uttering, and embezzlement.

- In 1977, the Secret Service, enforcing the forgery statute, successfully investigated and prosecuted William C. Siebert, an employee of the Department of Transportation who falsified vouchers and caused a computer to issue over \$850,000 in government checks which he converted to his own personal use.

In investigating computer related crimes involving sophisticated schemes, we are finding that the potential for computer abuse is limited only by the perpetrator's imagination. The cases investigated to date indicate that the law enforcement community has only scratched the surface. The National Chamber of Commerce estimates the yearly loss due to computer fraud at over \$100 million and experts have testified that only one out of a hundred instances of computer crimes are detected. The potential for lone felons, conspirators, organized crime, terrorist groups and even disgruntled employees is massive, and the accessibility is great. The risks are minimal and the payoffs are huge by historical standards averaging over \$450,000 per investigation.

The workload facing the law enforcement community is enormous. The Secret Service in meeting this challenge initiated and implemented a training program which introduces our agents to the computer environment and problems inherent in investigating and prosecuting computer related crimes. Our staff is currently working closely with Treasury Department officials involved with the direct deposit payment system in order to refine our investigative approach in the area of computer related transfers of government financial instruments.

Conclusion

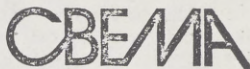
The Secret Service has already begun to play a role in this area as it relates to crimes involving government financial instruments. Our experience in investigating computer related crimes, as defined in S. 240, dictates that the Secret Service can and should make a significant contribution to the overall enforcement effort in the field. Passage of this bill will insure that the law enforcement community

will have an adequate tool to successfully investigate and prosecute computer related crimes. The Secret Service stands ready to meet these new challenges and welcomes the opportunity to continue our role as guardian of our nation's government financial obligations.

Computer technology is becoming integrated into nearly every aspect of human endeavor. The impact of this technology on Secret Service missions is inevitable and in keeping with our desire to maintain the highest possible level of professionalism we are prepared to exercise our investigative jurisdiction within the scope of S. 240.

While we recognize that some computer fraud legislation is contained in the comprehensive Criminal Code revision, we support the immediate passage of S. 240. In closing, I would like to thank the Committee for granting the Secret Service the opportunity to comment on S. 240 and request that we be afforded the privilege of expanding these comments if the Committee deems it appropriate.

Prepared Statement of CBEMA



February 27, 1980

The Honorable Joseph R. Biden
Chairman
Senate Subcommittee on Criminal Justice
Russell Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman:

The Computer and Business Equipment Manufacturers Association (CBEMA) is the principal representative for computer and business equipment manufacturers in the United States. CBEMA has followed the progress of the Federal Computer Systems Protection Act of 1979, S.240, since its inception as S.1776 in 1977. We support the overall purpose and intent of this legislation, and applaud the efforts of the Criminal Justice Subcommittee in reporting out what can be effective legislation.

Additional areas we feel the bill should address are the uses of personal computers or any devices with the capabilities to access or interface computer systems to carry out the intent of Section 1028 Computer Fraud and Abuses. Therefore, we suggest that in Section (2)(c) Definitions, the wording, input and output, be inserted immediately preceding the word logical. The sentence would then read: "For the purpose of this section, the term 'computer' means a device that performs input and output, logical, arithmetic, and storage functions by electronic manipulation..." And, that the language following the semicolon in Section (2)(c) Definitions, be altered to read: but does not include handheld calculators. There is also a need to extend coverage of this legislation to include remote access from outside the United States.

There is a distinct need for legislation in this area. The number of computers in use today commercially, by the general public, and by the Federal Government has grown drastically in the past decade. Consequently, the number of computer related crimes has also increased significantly.

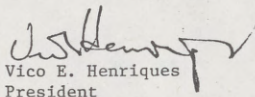
Today, there are eleven states which have enacted legislation on computer related crimes (Arizona, California, Colorado, Florida, Illinois, Michigan, Minnesota, New Mexico, North Carolina, Rhode Island, and Utah). Many more states have similar bills pending before their legislative bodies.

It would be in the best interest of the Government, the public, and the industry to have Federal laws which would at the very least, serve as a model to states considering enacting their own statutes.

We have every faith that you and your subcommittee will give this matter the careful consideration it deserves.

If CBEMA and its member companies can be of any assistance to you, please call upon us whenever necessary.

Sincerely,


Vico E. Henriques
President

VEH/bw

CC: Senator Edward M. Kennedy

EXHIBITS

Exhibit A - 1

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

JUL 21 1977

Honorable Elmer B. Staats
Comptroller General of the
United States
General Accounting Office
Washington, D.C. 20548

Dear Mr. Staats:

This is in response to your letter of June 17, 1977 and your draft report entitled "Computer Auditing in the Executive Departments: Is Enough Being Done?" We read the report with great interest and share your concern that internal audit groups throughout the Federal Government develop, maintain and effectively use capabilities for computer auditing.

The increasing use of computer and communications technology within the Federal Government has introduced a variety of new management problems. Among these is the need for assuring adequate management control over the automatic data processing (ADP) function. Auditing is an important tool used by agency management to monitor and control internal operations. We believe the ADP function should command more attention from agency managers for a number of reasons: (1) ADP impacts significantly upon virtually every aspect of an agency's operations, (2) by its nature ADP permits huge sums of money and large amounts of information to be handled by relatively few individuals, (3) computer users rarely have the ability or knowledge to verify the accuracy of computer systems, and (4) the large and rapidly growing cost of ADP itself.

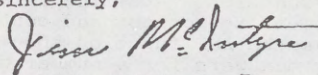
The Office of Management and Budget will continue to encourage agencies to establish adequate management controls, including audits, over their ADP operations. At the same time, we believe it is the prerogative of the agency head to make the basic assignments of audit responsibility within his agency and to make the priority decisions on the application of these resources. To assist agency management in carrying out the above, Federal Management Circular (FMC) 73-2 "Audit of Federal Operations and Programs by Executive Branch Agencies" was issued in September 1973.

As you know in recent months, in addition to this report, the General Accounting Office has issued two draft reports dealing with Federal Agency Audit operations: "An Overview of Federal Internal Audit" and "Need for More Effective Cross Service Auditing Arrangements." Both of these reports recommend OMB provide additional audit guidance to agencies and direct certain actions to be taken. GAO has also initiated a comprehensive review of internal operations in all the major departments and agencies with work currently underway in five agencies. Also, the recent General Accounting Office draft report "New Methods Needed for Checking Payments Made by Computers" contains recommendations affecting the audit process. In addition, the Joint Financial Management Improvement Program, which is a joint effort of the Treasury, OMB, the Civil Service Commission and GAO, is conducting a comprehensive study of Federal, State and local audit systems applicable to the Federal Assistance Programs. Since your report and these other detailed analyses seek to affect audit priorities and allocation of resources, we believe it is important that any additional guidance issued by OMB be in the context of a comprehensive picture of the Government's total needs and priorities. We believe these detailed analyses may provide us a basis for improving the guidance in FMC 73-2 and for working individually with the departments and agencies on improvements.

Since implementation of the recommendations in this report would rely heavily on agency participation, we would encourage wide dissemination of the final report throughout the executive branch. We understand from discussions with your staff that the four agencies cited in Chapter 2 of the report have undertaken action to correct the inadequacies reported.

Thank you for the opportunity to comment on the draft report.

Sincerely,



James T. McIntyre, Jr.
Deputy Director

Exhibit A - 2



COMPTROLLER

ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

24 AUG 1977

Mr. Donald Scantlebury
Director, Financial and General Management
Studies Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Scantlebury:

This letter responds to the GAO draft report dated June 17, 1977, "Computer Auditing in the Executive Departments: Is Enough Being Done?" We agree with the basic conclusions and recommendations to assure that the adequacy of audit coverage of ADP operations is periodically evaluated.

We fully appreciate the growing dependence on computers and the need for audits within the computer environment in view of the potential for (a) savings, (b) improved efficiency and (c) cost avoidance, and the need for better control of computer-based information systems. Since ADP is critical to many DoD operations, the mission of internal audit has been logically expanded over the past few years to cover computer auditing as discussed in the GAO draft report. The benefits from this expanded effort have been illustrated in the GAO draft report by inclusion of examples of audit results achieved by the Military Department audit organizations. We also recognize the need for increased oversight over ADP programs and we are taking steps to further improve audit services within DoD.

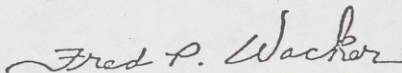
Under direction of my DASD (Audit), we have initiated a study within DoD (a) to review the nature and extent of internal audit coverage of ADP resources, (b) to define current performance, resources, skills and training problems associated with audit within the ADP environment and (c) to develop suitable overall DoD internal audit guidance for approaching audits of ADP systems and operations. We believe this study is in consonance with the intent of the GAO recommendations.

We noted one point of information in the GAO draft report which requires correction. On page 22, a reference to the Army Audit Agency review of the management and utilization of ADP equipment states that the audit was accomplished at 450 installations.

Actually, the Army had 450 installations which had computers when the cited audit was performed. Of these 450 data processing locations 16 were included in the selective audit.

We appreciate the opportunity to comment on this draft report and the observations furnished by your staff concerning computer auditing in the Executive Departments.

Sincerely,

A handwritten signature in cursive script that reads "Fred P. Wacker". The signature is written in dark ink and is positioned above the typed name.

Fred P. Wacker
Assistant Secretary of Defense

Exhibit A - 3



DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20410

July 21, 1977

IN REPLY REFER TO:

Mr. Henry Eschwege
Director, Community and Economic
Development Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Eschwege:

The Secretary has asked me to comment on the proposed draft report "Computer Auditing in the Executive Departments: Is Enough Being Done?"

The Department of Housing and Urban Development (HUD) has already recognized the need for increased emphasis in the area of computer auditing and the Office of Inspector General has taken aggressive action to meet this need. Since GAO contacted HUD on this review, we have recruited three experienced ADP auditors and developed an ADP training program for our audit staff. We have developed an approach to computer auditing that is tailored to the needs of HUD and the capabilities of our audit staff, with consideration of recommendations in prior General Accounting Office (GAO) reports.

Our approach to computer auditing recognizes that the impact of ADP on the Department's operations, expenditures and program accomplishments is more significant than direct expenditures for ADP resources. Consequently, we are emphasizing reviews of automated systems, both existing and under development. In addition, we anticipate significant reductions in manual audit work and increased audit coverage from the use of existing automated systems to support audits of program areas.

We evaluate our computer audit coverage annually when we develop our annual audit plan. We plan to increase our computer auditing as our training program helps us to develop the expertise necessary for this work. In the future, we plan to audit more automated systems and conduct more reviews to assure that ADP resources are used efficiently, economically and effectively.

Sincerely,

A handwritten signature in cursive script, appearing to read "James B. Thomas, Jr.", written in dark ink.

James B. Thomas, Jr.
Inspector General

EXHIBIT B : ANNUAL COST OF WHITE
COLLAR CRIME

(Billions of Dollars)		
Bankruptcy Fraud		\$ 0.08
Bribery, Kickbacks, and Payoffs		3.00
Computer-Related Crime		0.10
Consumer Fraud, Illegal Competition, Deceptive Practices		21.00
Consumer victims:	\$ 5.5	
Business victims:	\$ 3.5	
Government revenue loss:	\$12.0	
Credit Card and Check Fraud		1.10
Credit Card:	\$ 0.1	
Check:	\$ 1.0	
Embezzlement and Pilferage		7.0
Embezzlement (cash, goods, services):	\$ 3.0	
Pilferage:	\$ 4.0	
Insurance Fraud		2.00
Insurer victims:	\$ 1.5	
Policyholder victims:	\$ 0.5	
Receiving Stolen Property		3.50
Securities Thefts and Frauds		4.00
TOTAL (billions)		\$41.78

From the Chamber of Commerce of the United States, White Collar Crime Handbook, 1974

MISCELLANEOUS
 COMPUTERWORLD

More 'Stark Terror' Needed? Bankers Seen Unaware of EFT's Vulnerability

By Brad Schultz
 CW Staff

WASHINGTON, D.C. — More "stark terror" may be needed before the nation's bankers realize how vulnerable electronic funds transfer (EFT) systems are to unauthorized penetration.

So said Dan McCracken, president of the Association for Computing Machinery (ACM), at that organization's 1978 conference here recently.

Most who joined McCracken on a panel that pondered whether EFT is "moving too fast" for the people who manage such systems agreed that the recent \$10.2 million theft of funds from a Security Pacific bank in California through the Federal Reserve Systems EFT network, Fedwire, illustrated the inadequacy of most financial institutions' overall EFT security.

Charges of Apathy

The session also heard charges that most bankers are too ignorant or apathetic about data encryption and other methods of communications security, although panelist Arthur Hutt — A Bowery Savings Bank vice-president — remarked, "I don't think encryption

means a damn in Fedwire."

Security between nodes of an EFT network cannot prevent EFT crime if the nodes themselves are vulnerable to abuse, Hutt explained.

The Security Pacific episode exemplified this vulnerability, although it did not directly involve computer systems, he observed. According to police accounts, the perpetrator used a bank official's identity code to phone an order for the funds transfer, and the theft went unnoticed for eight days [CW, Nov. 13].

Site Security

The panelists seemed to agree that site security as well as communications security is a grave administrative problem for banks participating in EFT networks.

McCracken remarked that "some folks don't understand the ball game," indicating many bankers fail to appreciate that EFT can provide unparalleled opportunities for large dollar thefts while speeding funds transfer operations.

The federal government has failed to provide bankers with adequate guidelines and advice on EFT security,

McCracken suggested. Set up to provide this service, the National Commission on EFT ignored expert recommendations that DP professionals be included in its membership, he charged, indicating that the commission's findings were deficient as a result.

The ACM session heard a few "horror stories" of EFT abuse. For example, a Chicago bank reportedly mailed a customer her deposit/withdrawal card and personal identification number to empty her \$600 account and create a \$1,200 overdraft.

Under the Financial Institutions Regulatory Act recently signed by President Carter, unsolicited debit cards, but not unsolicited PINs, may be mailed to bank customers, according to Pender McCarter of the American Federation of Information Processing Societies (Afiaps) Washington office. The law also limits access to financial records by federal authorities and sets other privacy rules [CW, Oct. 23].

McCarter cited computer crime expert Donn Parker's testimony before the U.S. Senate that raised banking as the leading area of such abuse (20% of

all computer crime), followed by the federal government (17%) and education (15%).

McCarter agreed with Parker that "the automated teller machine [ATM] is potentially the most vulnerable computer terminal" and is especially attractive to would-be felons, including those in the Mafia.

Risks Minimized

"Bankers seem to minimize the security risks associated with ATMs," McCarter told the session. He referred to a recent American Banking Association survey of banks using ATMs which stated that most banks claimed "no security problem at all or considered their security as extremely effective" [CW, Dec. 11].

The National Commission on EFT's final report, issued last year, maintained that "few breaches" were found in EFT security, McCarter continued.

The Afiaps research associate called upon computing professionals to "address the problem of DP crime by offering realistic estimates of the reliability, security and accountability of present and future EFT systems."

Rational Assessment Welcome

A "rational assessment" of the federal Data Encryption Standard (DES) — which critics have called breakable — would be especially welcome, he indicated.

"Certainly such information as that provided by Frank Backman of IBM's Washington Systems Center that a fully integrated, large-scale, on-line EFT system is still beyond the state-of-the-art" is extremely useful for planning purposes," he said.

McCarter concluded with an outline for studying EFT issues, adapted from a proposal by Prof. Rob Kling of the University of California at Irvine:

- 1.1 Definitions & Relationships
- 1.2 Technical Issues
 - 1.2.1 Reliability
 - 1.2.2 Security
 - 1.2.3 Auditability
 - 1.2.4 Implementing EFT
- 1.3 Standards
- 1.4 Legal/Regulatory Issues
- 1.5 Social Issues
 - 1.5.1 Privacy/Confidentiality
 - 1.5.2 Quality of Life

THE COMPUTER FRAUD

WEDNESDAY, FEBRUARY 20, 1980

© 1980, Washington Post Co.

U.S. Aide Held in \$500,000 Theft by Computer

By Chris Schauble
Special to The Washington Post

BALTIMORE, Feb. 19—A worker at the Social Security Administration headquarters was charged today with manipulating the national computer at the complex in order to pay herself and two accomplices more than \$500,000 in disability benefits.

The computer, in the Baltimore suburb of Woodlawn, sends out \$1.1 billion in disability checks each month to workers and their dependents each month. The Secret Service, which spent 18 months unsuccessfully trying to trace the money stolen through false disability claims, today described the

computer theft scheme as "very, very sophisticated."

"If there hadn't been a bank official in Philadelphia alerted to a discrepancy in an account opened there, we'd still be operating in the land of the unknown," said Andrew E. Berger, head of the Secret Service office here.

"This was a very sophisticated scheme and the potential of a loss of use of the computer is a real one," said Berger. "There's a potential [that] we're sitting on the tip of an iceberg with this." He said agents from Washington, Philadelphia and California are continuing the investigation.

John Trollinger, a spokesman for Social Security, said, "There are safe-

guards in place and we are continuously reviewing and revising our computer system."

The worker is accused of processing disability checks under numerous aliases, using real social security numbers and then erasing all records of payments from the computer before it produced a regular audit of claims and payments, Berger said.

Blair, 29, who has worked at the agency since 1973, allegedly operated the computer theft scheme by filling out the paperwork for the computer to send disability checks to various addresses and post office boxes in Washington and Philadelphia. The accomplices allegedly used the checks, cashed them through savings

accounts with several banks, and, a short time later, closed out the accounts, Berger said.

None of the money allegedly obtained from the scheme has been recovered, investigators said.

Blair was arrested last week in Baltimore while selling in sick to her office. She is still employed at the Social Security Administration, and a spokesman there said Blair "was transferred to a nonsensitive position as a result of the investigation."

She was ordered jailed in lieu of a \$100,000 bond by a federal magistrate following her indictment on 46 counts of conspiracy to defraud, and on 46 counts of fraud. She was made an aid-infraud abetting charge.

Stella Marie Abrams, 31, of Phila-

delphia, and Malcolm Blair, 29, Blair's brother-in-law, were charged as accomplices in the indictment returned by a federal grand jury here today. Malcolm Blair is charged with conspiracy in Pennsylvania on an unrelated charge of receiving stolen Treasury checks.

Assistant U.S. Attorney David Queen said at the bail hearing for Janet Blair that she was "not acting alone" in the scheme and "may have been taking orders from members of a religious sect who acknowledged that any suspicion about what happened to the half-million dollars allegedly stolen in the computer fraud scheme are just suspicions.

The Evening Sun

BALTIMORE, MARYLAND

TUESDAY, FEBRUARY 19, 1978

Three indicted on charges of defrauding SSA

By Frank Kauffman

An employee of the Social Security Administration in Woodlawn and two other persons were indicted by a special federal grand jury today on charges of stealing about \$500,000 by rigging a government computer to send disability checks to phony beneficiaries.

The U.S. Treasury checks—in most cases amounting to several thousand dollars each—were allegedly deposited in bank accounts two of the defendants opened under assumed names in Philadelphia and Washington.

Indicted today were Janet B. Blair, 29, of Baltimore, a benefit authorizer at Social Security's former Bureau of Disability Insurance; her brother-in-law, Malcolm Blair, 29, currently serving a federal prison sentence on unrelated charges; and Stella M. Abrams, 31, of Philadelphia.

The alleged scheme, which lasted from January 1978 through last November, resulted in scores of disability checks being sent to fictitious beneficiaries in Pennsylvania, Maryland and Washington, according to the 43-count indictment.

All three defendants were charged with conspiracy to defraud the government. Ms. Blair also is charged with 21 counts of making false Treasury checks and another 21 counts of aiding in the forgery and passing of the forged checks.

Andrew E. Berger, special agent in charge of the U.S. Secret Service in Baltimore, said disclosure of the scheme pointed up that the "potential for misuse and the lack of safeguards at Social Security in Woodlawn is alarming."

"There seems to be a lack of checks and balances and controls in their procedures" and audits, he complained.

The 18-month investigation by the Secret Service that led to today's indictment is continuing, and Mr. Berger said he was not yet certain whether the case represents what may be only a small part of a much bigger problem.

A spokesman for Social Security said the administration had not seen the indictment papers and would have no comment.

Social Security issues \$1 billion in disability payments each month. Ms. Blair's job was to process payments for approved disability claims.

According to the charges, Mr. Blair and Ms. Abrams used phony identifications to open several accounts at a savings bank in Philadelphia and two banks in Washington.

They then allegedly gave the names

and mailing addresses to Ms. Blair at Social Security.

Using genuine Social Security account numbers, Ms. Blair allegedly created fictitious beneficiaries with the names and addresses provided by the other defendants.

The false information was fed into a

3 indicted in SAA scheme

[Continued from Page A 1]

computer at Woodlawn which put out computer tapes with the names of the phony beneficiaries, according to the indictment.

The tapes then went to a Treasury Department office in Philadelphia and "were then used to create seemingly authentic Treasury checks which were thereafter mailed to the fictitious payees at the designated addresses," the indictment said.

The computer, according to the indictment, failed to detect the phony beneficiaries because the computer system relies on account numbers and not names.

Mr. Blair and Ms. Abrams allegedly deposited the government checks in the various bank accounts.

"Eventually, the accounts were depleted and the funds disbursed to unknown locations," the indictment said. The accounts now contain virtually no money, one source said.

Ms. Blair, a Social Security employee since 1973, allegedly covered up the scheme by directing the computer to erase all records of the phony transactions, "thereby not interrupting benefits to the legitimate account holders."

The grand jury said it did not know the exact amount of the fraudulent disbursements, but said it believes it to be about \$500,000. Ms. Blair was charged in connection with 21 phony checks, but investigators are not sure exactly how many checks were sent out in the scheme.

Mr. Berger of the Secret Service said the continuing investigation is focusing on the Baltimore, Philadelphia and Washington areas but may also reach California.

He said the investigation began when a Philadelphia bank official became suspicious about a savings account Ms. Abrams opened in 1978. The banker notified the Secret Service because the woman had attempted to deposit a government bond into the account, he said.



BALTIMORE, WEDNESDAY, FEBRUARY 20, 1958

Woodlawn worker said to defraud U.S. of \$500,000 in fake disability payments

By SHERRILL LYONS

A Social Security employee was charged by a federal grand jury yesterday with defrauding the government of \$500,000 in disability payments to nonexistent beneficiaries in an apparently unprecedented computer-fraud scheme.

The grand jury indicted the 800 block North Rosebush street, a benevolent society, and its authorized administrator in Woodlawn, is charged with conspiring to defraud the government and making false U.S. Treasury checks from

January, 1978, until last November.

Andrew E. Berger, the agent in charge of the Baltimore office of the Social Security agency, said the "money substitution" scheme "is the first case we know of using computers" to defraud the Social Security system, whether or not agents at the tip of the iceberg right now, we don't know," Mr. Berger said. "The potential for misuse of taxpayers' funds and the inner working of the Social Security is not known to us, but we know that it is there."

Mr. Berger said the investigation revealed a lack of checks and balance and controls in their procedures. "The system is so complex that it is almost alarmingly so," he said.

The office involved, formerly titled the Bureau of Disability Insurance, issued checks on a month in disability payments. Mrs. Blair allegedly used two co-defendants to receive, deposit and withdraw

See BENEFITS, A6, Col. 3

Social Security aide accused of cheating U.S.

ALBERT BENEFITS, from Alameda, Calif., was charged yesterday with defrauding the Social Security Administration of \$500,000 in disability payments to nonexistent beneficiaries in an apparently unprecedented computer-fraud scheme.

The grand jury indicted the 800 block North Rosebush street, a benevolent society, and its authorized administrator in Woodlawn, is charged with conspiring to defraud the government and making false U.S. Treasury checks from

the payments, which have not been recovered. Mrs. Blair, who has worked at the agency since 1973, was responsible for computerizing the Social Security system. She is accused of taking genuine Social Security numbers and using them as fictitious beneficiaries on computer tapes for those numbers—in names being used by the alleged co-defendants to open accounts in Washington and Philadelphia.

Mr. Berger said the investigation revealed a lack of checks and balance and controls in their procedures. "The system is so complex that it is almost alarmingly so," he said.

The office involved, formerly titled the Bureau of Disability Insurance, issued checks on a month in disability payments. Mrs. Blair allegedly used two co-defendants to receive, deposit and withdraw

See BENEFITS, A6, Col. 3

reversing our computer system and add. The Secret Service was called in to investigate the case. Mrs. Blair, who has worked at the agency since 1973, was responsible for computerizing the Social Security system. She is accused of taking genuine Social Security numbers and using them as fictitious beneficiaries on computer tapes for those numbers—in names being used by the alleged co-defendants to open accounts in Washington and Philadelphia.

Mr. Berger said the investigation revealed a lack of checks and balance and controls in their procedures. "The system is so complex that it is almost alarmingly so," he said.

The office involved, formerly titled the Bureau of Disability Insurance, issued checks on a month in disability payments. Mrs. Blair allegedly used two co-defendants to receive, deposit and withdraw

See BENEFITS, A6, Col. 3

Computers

Where crime escapes the law

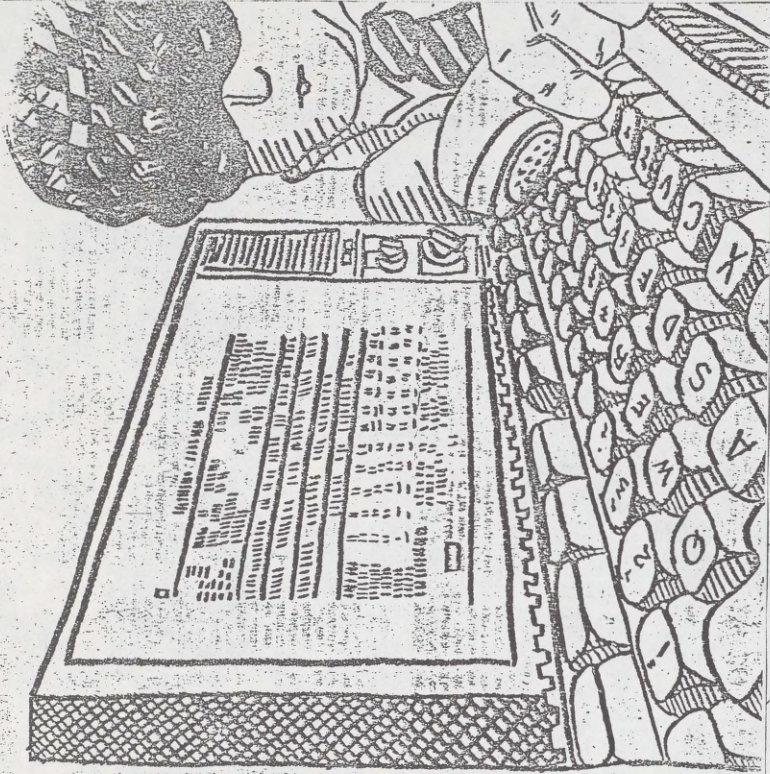
By W. H. EARLE

If you're planning to commit a computer crime, better do it before it becomes illegal.

Can a crime be legal? It can if no law against the "crime" has yet been passed—having government prosecutors with no means of punishing the criminals.

That is precisely the situation confronting state and federal prosecutors with regard to the relatively new field of computer crime. Consider:

Virginia's blueprint conceals its predicament by stating that a computer crime is defined "in a nongraphic computer tape. Lacking a more specific law, the prosecutor considers using a vandalism statute to charge



Baltimore Sun, 12/18/79

... not every act of
computer abuse is

... not every act of computer abuse is free of peril for the perpetrator.



With no statutes, prosecutors can't charge those who use computers illegally

malicious destruction of property. However, research indicates that the data are not property at all. Several courts have held that the "intangibility" required to constitute "property" under the law, if the data were not property, then nothing was destroyed. The charge is dropped.

Charges are also being developed based terminal in his home to tap his former employer's computer. He prints out a copy of a valuable program on his home terminal, then makes the program available to other terminals. The program is copied. Has the analyst committed larceny? Not at all: since the program was only copied, it is still available in the former employer's computer. Nothing, therefore, has been destroyed.

According to the law, the developing field of computer law, the examples above illustrate only two of the many loopholes in the current law applied to computers. The first example occurred in Colorado in 1974. A computer programmer was charged as soon as an unscrupulous programmer finds it in his interest to carry out the "crime".

Given the pervasive influence computers have in the quarter-century since their introduction, attention is being focused on their susceptibility to criminal manipulation. According to reports in *Computerworld*, the litigation trade journal, seven states have enacted computer crime laws in the past two years, all intended to close the gaps.

Mr. Earle, a Baltimore free-lance writer, works in the planning department at a federal data processing installation.

met in the law by rapidly developing technology. At least half a dozen other states are considering similar laws. At the federal level, the Senate Committee on the Judiciary is now considering the Federal Computer Crime Control Act of 1974, which defines crimes related to federal computers, to computers operated by financial institutions and to computers operating in interstate commerce.

Every act of computer crime, of course, not only has a perpetrator, but also a victim. Susan H. Nyman, a California computer-law researcher, identified more than 40 federal laws which conceivably apply to computer crime. She says that the statutes on theft, communication, espionage, burglary and various types of fraud. The states have their own arrays of statutes which cover a wide range of offenses in state legislatures.

The problem with all these laws, however, is that none was written with the computer in mind. Thus the ingenuity of "hobnobbers" is tested as they try to find definitions crafted long before the computer came on the scene.

For example, when an attempt was made in 1970 to destroy a computer index of 100,000 names, a computer programmer, which Mr. Nyman was suing for, filed

covered that the would-be saboteurs could be charged only under a statute prohibiting a misdemeanor. The absence of more appropriate statutes accounts for the rash of new laws under consideration.

What, unfortunately, refining the statutes which define computer crime is only a part of the problem. The more difficult part is detecting that a crime has taken place.

Computer crime is unique in that the act may take only milliseconds of a second, magnetic charges—"clones" of which remain in the loaded machine. Even when some more tangible asset is involved—money, for example, or products from a factory—there is no way to trace the money to donor. The computer record so that intricate and painstaking audit is required even to establish that a crime has been committed.

It is possible that many computer crime experts in the field have not come to light, through systematic applications of security procedures, rather, the electronic crooks have been tripped up by unscrupulous computer users.

Thus a bank teller in New York survived three years of routine audits by juggling accounts to conceal an embezzlement of \$1.5 million; he was caught only when a raid on his books revealed that he

had been betting up to \$30,000 a day on horse races.

A consultant in Maryland made a fortune in the computer business by using a phone in the computer of his former employer. The arrangement collapsed only because the former colleague walked into the computer room while the computer was operating and saw the man supposedly working at a remote location.

The fear nagging at security experts is this: If a substantial number of computer crimes have been detected only by accident, perpetrated by the experts—going undetected? No one knows.

Furthermore, how much "is" being stolen? All figures are questionable because of the difficulty of tracing the money. It has been broken, but a few figures are useful, and a number of estimates have been made.

A study by Don B. Parker of the Stanford University School of Business in 1968 and 1971, accounting for \$280 million in losses. However, in testimony before a Senate subcommittee in 1973, Mr. Parker cited without comment the U.S. Chamber of Commerce's 1971 estimate of \$100 million a year. Other credible sources have offered estimates up to \$300 million a year. The fact, that no one knows,

What is known is that opportunities for computer crime will increase as the number of computers increases. There are more computers in the United States today and the number grows each year. Also growing is the number of workers tending the machines, many of whom are fresh-learned graduates of high school and college. The potential computer criminal, many of whom fit neatly into Mr. Parker's "profile" of the potential computer criminal.

Young, bright and highly motivated, the computer criminal has the technical competence to assume the highly sophisticated "perfect crimes" which theoreticians insist can make a mockery of any known computer security system. Since the computer is a machine, it can be broken 60 times as fast as the average bank robbery, the stakes are very high.

Furthermore, until fairly recently, would-be computer criminals had a substantial number of "back doors" in the early years of automation, auditors government-lawyers and police officials tended to recall from an incomprehensible world where bank accounts, inventories and people were all selected alike to more or less be checked. The computer operators were often disinclined to worry about security or internal accounting requirements. They took money but they did not help in meeting production schedules.

Only in this decade have attitudes begun to change, as more and more remarkable crimes have come to light. Major auditing firms now insist on dealing transactions through all the computer's internal operations. Federal and state law enforcement officials are attending data processing courses sponsored by the Federal Administration.

The data processing industry has improved its own security measures, too: Access to systems is controlled; data transmissions are encrypted; programs and archives of security clearance which limit the actions particularly individuals are authorized to take.

Such progress, most security experts believe they will be able only to limit losses, not eliminate them; controls devised by the ingenuity of man can be undone with the same ingenuity. A few years ago, for example, computer operators were able to "unbreakable" system to protect data in computers being used by the Defense Department.

As a test, two computer specialists were invited to try to crack a computer system. The time required to penetrate the system, rob its files and create a permanent treasury path for the saboteur? A little less than two weeks.

Don B. Parker

The document and articles follow:

AMERICAN BAR ASSOCIATION,
Chicago, Ill., September 11, 1979.
Re Jurisdiction over crimes committed
against or through use of computers.
Hon. ABRAHAM RIBICOFF,
U.S. Senate,
Washington, D.C.

DEAR SENATOR RIBICOFF: At the meeting of the House of Delegates of the American Bar Association held August 14-15, 1979 in Dallas, Texas, the attached resolution was adopted upon recommendation of the Section of Criminal Justice. The action taken thus becomes the official policy of the Association in this matter.

This resolution is transmitted for your information and whatever action you may deem appropriate. Please do not hesitate to let us know if you need any further information, have any questions or if we can be of any assistance.

Sincerely yours,

F. WM. MCCALPIN.

RESOLUTION

Be it resolved, That the ABA support legislation to establish federal jurisdiction, concurrent with state jurisdiction, over certain offenses committed against, or through the use of computers, computer systems or computer networks;

Be it further resolved, That the proposed federal concurrent legislation reach:

(a) the use or attempted use of a computer, computer system or computer network to obtain money, property or services by means of false or fraudulent pretenses, representations or promises;

(b) intentional, unauthorized accessing for the purpose of alteration, damage, destruction or theft of a computer, computer system, computer network or any computer software, program or information contained therein;

(c) intentional, unauthorized interception of nonaural communications by wire or radio between computers, computer systems, or computer networks;

Be it further resolved, That legislation creating concurrent federal jurisdiction over offenses committed against or through the use of computers, computer systems or computer networks require the Attorney General, in consultation with state and local enforcement authorities, to publish guidelines for the exercise of that jurisdiction by the United States;

Be it further resolved, That legislation denominating federal offenses committed against, or through the use of a computer or computer systems or computer network should:

(a) preclude the charging of a federal offense based upon the same facts except for proof of an element involving a computer, with a charge brought under the computer crime statute;

(b) provide for gradation of offenses and a graduated scale of penalties consistent with ABA policy on the sentencing scheme of the proposed Federal Criminal Code, with a sanction not to exceed five years imprisonment or \$50,000 or both; and

Be it further resolved, That additional study be undertaken to find solutions to the procedural and evidentiary problems that impede the detection and prosecution of computer crimes under existing law.

[From the New York Times, Sept. 27, 1979]

TECHNOLOGY COMPUTERS AND CRIMINALS

By Peter J. Schuyten

The setting: a quiet university town somewhere in the Northeast. An "intruder" electronically penetrates the operating system of the town's centralized data processing center. After causing a series of bizarre ac-

idents, the interloper threatens to "crash" the system, throwing municipal services into chaos unless a \$ million ransom is paid and electronically transferred to a numbered bank account somewhere overseas.

Fanciful? Not really. According to experts in the field, Louis Charbonneau's novel of computer crime, "Intruder," could indeed happen. They say that such a scenario is technically feasible—and easier than most people realize.

According to a Government report a few years ago, anyone with the right background in computer sciences and, say, nine months of working experience on a particular operating system could conceivably take over the system, using it to work against itself. Some experts say it would not even take that long.

"Software systems aren't perfect," says Theodore M. P. Lee, manager of system security for the Sperry Univac division of the Sperry Rand Corporation. "If someone really put his mind to it, he could take over a system. He might have to work at it a bit, but he could get into a position where he could read the computer's files and even change them, using the power of the computer against itself."

Stanley Mark Rifkin stole 10.2 million from California's Security National Bank in less than an hour. He knew enough about computers to crack the bank's software codes, causing the money to be transferred to an account in a New York bank, whereupon it was sent to Zurich and used to buy diamonds.

Mr. Rifkin was caught, but the experts suspect that most computer crime goes undetected or even unreported for fear of the embarrassment it would cause and the difficulty in making a prosecution stick.

"We only read about the failed computer criminals," says Robert A. Jacobson, president of International Security Technology Inc., a computer security consulting concern, adding, "The really successful ones are never really detected in the first place."

Security is an issue that many computer users apparently prefer to ignore. It is complicated and expensive. "The typical company doesn't really care about security," says Larry Wells, president of Creative Strategies, a market research firm.

With the rapid proliferation of computers, and in particular the trend toward distributed data processing (where a number of terminals are hooked by communication lines to a large central processor), companies are highly vulnerable not only to crimes such as fraud and theft of trade secrets but also to the accidental loss of valuable financial operating data through malfunctions, fire and the like.

What can the computer user do? Most computer manufacturers build a certain level of security into their software. "You already get some of the mechanisms you need to restrict access to files in data banks," says Mr. Lee of Sperry Univac. "The difficulty is getting people to use them."

Beyond that, there is physical security, including a backup power system, air-conditioning, automatic fire detection and extinguishing, and a secure, usually computerized, locking system. The computer companies will usually supply a list of architects and contractors who specialize in facilities of this kind.

For minicomputers and intelligent terminals, Transaction Security Inc. of New York has recently developed a portable self-contained enclosure that provides these features.

For systems that use communication lines, backup lines to the telephone company central office are usually recommended, and devices that scramble data at one end and reassemble at the other end may be necessary.

S. 240 IS VOTED OUT OF CRIMINAL JUSTICE SUBCOMMITTEE

Mr. RIBICOFF, Mr. President, the Subcommittee on Criminal Justice of the Judiciary Committee has voted out S. 240, the Federal Computer Systems Protection Act.

As the author of this bill, and in behalf of Senator PERCY and other sponsors of this legislation, we express our appreciation for the consideration given the measure by the subcommittee chairman, Senator BIXEN, and other members of the subcommittee. I am hopeful that the progress that has been made will continue and that S. 240 will go forward in the legislative process.

Mr. President, I request that the following documents be printed in the RECORD: A letter from F. William McCalpin, secretary of the American Bar Association, accompanying a resolution adopted by the House of Delegates of the ABA meeting in Dallas, Tex., on August 14 and 15, 1979, regarding computer law; an article from the New York Times of September 27, 1979, by Peter J. Schuyten; an article from Canadian Business by Lydia Dotto; an article from the Los Angeles Times of August 20, 1979, by Craig Turner; an article by Angeline Pantazes and an article by Vin McClellan from the August 1979 issue of Dun's Review.

Beyond that, the concerned user can hire a consultant. Mr. Jacobson of International Security Technology, for example, has developed a software program called Ramp that evaluates security risks of an installation and assesses the cost of additional protection. Then too, most of the "Big Eight" accounting firms have consulting arms that provide periodic audits of how secure a data processing system is.

"This is not a once-a-year assessment, a temperature taking, but rather an ongoing identification of threats and shortcomings," explains George H. Pittersbach, a principal at Peat, Marwick, Mitchell & Co. He says: "What most people overlook is that this is a changing process. You add a terminal here, people with passwords there, or alter the software."

In addition, there are companies that specialize in what are known as "software locks," programs costing between \$5,000 and \$15,000 that are designed specifically to protect computer systems from unauthorized use by outsiders and even by insiders. One such company is Pansophic Systems Inc. of Oak Brook, Ill.

Then too, there are programs called audit trails, which record every entry into a system, the user, the nature of the transaction and the length of time the terminal was used.

For very large computer users, there are backup facilities available to avoid a system crash. Companies such as Sun Information Services of Valley Forge, Pa., or Contingency Group Inc. of Bensenville, Ill., provide such services—for \$2,500 to \$4,000 a month.

Finally, some companies, particularly those providing time-sharing services such as the General Electric Information Service Company, use "computer busters." One of these is the System Development Corporation of Santa Monica, Calif. Its job is to try to break into their computer systems.

THE NEW COMPUTER CRIMINALS—MOUNTING LOSSES TOTAL \$300 MILLION ANNUALLY

(By Lydia Dotto)

Shortly before midnight on Aug. 26, 1977, five men crept stealthily into the University of Alberta's Agriculture Building and made their way to Room 274. There they bagged their long-sought quarry—a young man industriously working at a computer terminal. "He was speechless," recalls Dale Bent, U of A's director of computing services.

For nearly a month, Bent and his staff had, with mounting frustration, been tracking an elusive meddler who was causing crashes of the university's \$5-million computer system, disrupting the work of some 5,500 authorized users. On Aug. 19, as staff members tried to put material into the memory banks from magnetic tapes, the meddler, working at a remote terminal, promptly wiped it out.

Bent and his colleagues then brought the computer's ability to monitor the activities of its users into play. They pinpointed a terminal in the Agriculture Building and discovered the nineteen-year-old meddler. Last December he and an accomplice were convicted of mischief and theft of a telecommunications facility. They received suspended sentences and were put on probation because tampering "had not been for financial gain."

This was Canada's first computer fraud case in court, but there is no doubt the computer will figure prominently in the future world of crime. Information is a tangible, salable commodity; information is power; information is money.

The computer is the most effective and versatile repository and processor of information the world has ever seen—except, perhaps, for the human brain. A 1977 report for the Organization for Economic Cooperation and Development (OECD) suggests that by the end of the next decade "most recorded

information . . . will be in computer-readable form."

More than mere storage of information is at issue. The computer is a powerful tool for reorganizing and selecting information. As the OECD report notes, "The evaluation of a vast quantity of information imparts a new and potentially more dangerous quality to it." Moreover, the ease with which data banks can be tied together increases the likelihood of unintended use of information.

This has prompted concern about the proliferating use of social insurance numbers by governments, banks, and private business. When all the educational, financial, medical, etc.—carry a single identifying number, can the electronic dossier be far behind?

Computer information can be reproduced instantly and can be transmitted over telephone lines. The central data base can be penetrated from afar by people using remote terminals. Computer fraud expert, Donn Parker of the Stanford Research Institute says, "The criminal no longer has to be at the site of the crime. Theoretically, if he has access to a telephone in Outer Mongolia, he can instantaneously commit a computer crime here in Toronto."

An estimated \$300 million is lost worldwide each year through computer abuse, but there is no way of knowing exactly how much the careful thieves who haven't been caught are getting away with. Many companies, fearing embarrassment and a loss of reputation, prefer to deal with computer crimes quietly. And the inadequacy of laws dealing with such technological crime makes convictions rare.

Computer crime falls into three categories: theft of computer time; manipulation or destruction of computer information—particularly financial information—for personal gain; and theft or unauthorized use of information stored in computers. Theft of computer time occurs when employees or students use the computer for personal and often frivolous purposes, such as calculating mortgage payments or drawing Snoopy cartoons. Such use is ubiquitous and is not generally considered a serious problem.

Theft of money by manipulating financial data banks is the most publicized of computer crimes. In the tradition of spectacular heists, there's an element of art to the more clever computer-assisted thefts, with none of the heavy-handedness involved in marching into a bank totting a gun. Stanley Rifkin, a California computer consultant, stole \$10 million from a bank by means of a 10-cent telephone call using his knowledge of the bank's wire system to transfer money. There is also what Donn Parker calls the salami technique: "stealing small slices of money from a large number of accounts so that nobody notices."

Our present rate of theft by computer will pale if and when electronic funds transfer—the so-called cashless society—becomes a reality. Data then will become money, and the potential for what one consumer advocate calls "remote mugging" becomes staggering.

Stealing money is not the only way in which financial data banks can be abused. They can be altered for personal gain (someone could change a computer file to reflect a good credit rating). Or they can be used—along with medical, educational, criminal, welfare, and other data banks—for purposes not intended when the data were collected. Hearings last year into Royal Canadian Mounted Police activities revealed that the Mounties had almost unlimited, if under-the-counter, access to the central computer index of social insurance numbers. They not only had used the information to track down suspects but also had shared the data with other police departments. Tax, customs, and immigration officials, also had access to

the file. The Government stopped this practice last year but announced it wanted to legalize police access to the file.

No definition of privacy is universally accepted, but in the context of computer crime two recurrent elements emerge. First, individuals should be able to find out what kind of personal information is being stored and whether it is accurate; second, they should be able to find out who has access to the information and, to some extent, to control its dissemination.

There are still other concerns relating to computers. One is that the individual has a harder time leaving his past behind: a computerized record can pursue him to his grave and even, through loss of reputation, beyond. Another problem arises from the ability to link computer files together, which makes surveillance of an individual's activities infinitely easier.

These concerns, along with the growing incidence of computer-related crime, have intensified the quest for the uncrackable computer. Most new techniques are designed to increase the "work factor"—the amount of work required for an average programmer to penetrate the system. "Perfect security is never obtainable," notes the OECD report. "The most that can be achieved is a 'work factor' so long that it deters would-be infiltrators."

According to Dale Bent, the man who helped catch the student computer thief, the kind of security system in use on the University of Alberta computer (which he says is superior to those commonly used in industry) requires inside knowledge and expertise to crack. Thus, though it provides good protection against unskilled users, on a university campus "it must be assumed that there are many users with the expertise to commit violations. . . . Judged by this standard, security cannot be excellent."

Computer experts agree that there is, as yet, no impenetrable computer. It's not uncommon for university students to undertake computer-cracking projects as class assignments. In 1976 the U of A system was plagued by the use of a program that reduced the charges assessed for computer time. The program, developed as a course project by a computing sciences student, somehow got into the hands of several users.

One of the major problems in computer security is finding ways to prevent abuse by legitimate users. This is why technological barriers are not enough; one expert estimates that only one in 500 computer crimes would have been prevented by sophisticated encrypting codes.

John Carroll, a computer science professor at the University of Western Ontario, queried fifty third-year computer science students—anonymous, of course—and found that 34 per cent had tried to penetrate the security of the system; 20 per cent had tried intentionally to crash it; 34 per cent had tried to obtain computer time without paying for it; and 28 per cent had used a talk circuit to harass other users. Carroll emphasizes that the computer in question is used exclusively for teaching and research, and that "there's nothing worth stealing in it."

Would the students have refrained from crashing the system if the computer had contained anything worth stealing? "I'd like to believe so, but I wouldn't bank on it," he says. Many of the students believed they weren't doing anything wrong, unless they were harming an identifiable individual. Cheating a large organization didn't seem to count.

Carroll was alarmed to find a high correlation between competence and an inclination to engage in questionable behavior—probably because of the challenge involved. "The better kids, the smarter kids, are more likely to do it," he says. For the business world, that's a rather ominous conclusion.

Carroll is trying to devise a test containing seemingly innocuous questions that could pinpoint high-risk individuals. Such a test might weed out most potential computer abusers, but it could also weed out many of the brightest and most talented applicants. So far, Carroll is successful; companies might not use his test. Genuine talent has been so hard to find that industry has tended not to ask too many questions.

The idea of background checks inevitably raises questions about civil rights, but Donn Parker says, "You have to balance civil rights with society's right to security. I think there's a reasonable balance. People in a position of trust must anticipate their backgrounds will be known."

Like many other experts, Parker believes that licensing, accreditation, or certification can do much to establish a minimum level of competence—but can't guarantee honesty. University of Toronto computer expert G. G. Gottlieb believes that licensing would have little impact, unless removal of the license or certificate would prevent the person from his livelihood. Certificates now can be obtained by passing an examination administered by the Institute for the Certification of Computer Professionals, but computer operators and programmers can work without them.

But even if there were professional regulation, it seems doubtful that this would entirely stifle human ingenuity—or larcenous inclinations.

[From the Los Angeles Times, Aug. 20, 1979]
SECURITY FOOK: COMPUTERS AN EAST TARGET

(By Craig Turner)

Computer experts like to tell the story of the office worker who discovered he could print multiple copies of his company's paychecks simply by pressing the "repeat" button on the firm's computer.

Until he was turned in by a suspicious bank teller, the employee illegally inflated his salary by printing as many as 200 duplicates of his regular paycheck.

That anecdote, drawn from the files of computer security specialist Donn Parker, shows that not all computer crimes require extensive technical know-how.

Others, however, can be far more sophisticated, more lucrative and less easily detected. And as American businesses, consumers and government agencies become more reliant on computers, the potential for fraud and theft increases enormously, according to a growing number of experts.

"It's not currently possible to build an adequate, technically secure computer system," said Parker, senior consultant at SRI, Inc. (formerly Stanford Research Institute) in Menlo Park and author of the book, "Crime by Computer."

"Even if we did know how to design and produce a technically secure computer system, that's not the problem. It's the environment in which the computer is used. . . . Even when they (computer customers) get all the security systems, they find it sometimes interferes with the use of the computer, so they don't use the security."

Meanwhile, most law enforcement agencies are admittedly unprepared to deal with the growing problem. While police for years have used computers to help catch criminals, they seem hard pressed today to catch criminals who use computers.

"We really haven't trained our investigative apparatus in computer crime, or white-collar crime, for that matter," said Washington lawyer August Bequa, a former federal prosecutor now in private practice. "By and large, our police forces are defenseless in this area. The leadership in our police forces haven't been interested. . . . Prosecutors are

no better. They don't have any training either."

Authorities are beginning to recognize the problem, however.

There is a waiting list for classes in computer crime at the FBI Academy in Quantico, Va. Students there have included police detectives, federal investigators and representatives of Scotland Yard and the Royal Canadian Mounted Police as well as FBI agents.

The Federal Law Enforcement Assistance Administration is planning this year to fund a \$400,000 training center in computer crime for local prosecutors and investigators. Five states have adopted laws aimed specifically at computer crime and bills are pending in the California Legislature and in Congress. In Los Angeles, the district attorney's office has set up an electronic crimes section without in the major frauds division, and the California District Attorney's Assn. sponsors the National Computer Crime Data Center.

Business has been slower to react. "It's been treated as a minor technical matter when it's really a major corporate problem," said Robert P. Campbell, president of a Woodbridge, Va., computer security firm.

No one knows the precise cost of computer crime in America. The FBI estimates the average loss from a computer crime as \$620,000. The U.S. Chamber of Commerce places the annual total at \$100 million. Parker, who has files in 680 cases, said the figure may be as much as \$300 million annually, but classifies all estimates as "guesstimates" because only a small number of computer crimes—perhaps fewer than 15%—are reported to authorities.

The potential earnings of electronic fraud are starkly illustrated by Parker's study of computer-aided bank embezzlement, however. In an interview, Parker said that while FBI statistics for all embezzlements show an average take of \$19,000, his review revealed a loss of about \$450,000 in the typical computer-related embezzlement.

Last year, Stanley Mark Rifkin, a Los Angeles computer analyst, used his knowledge of a secret fund transfer code to impersonate a bank official and steal \$10.2 million from Security Pacific National Bank. Rifkin pleaded guilty and was sentenced to eight years in prison last March.

Computer crimes, however, cover a broad spectrum, ranging from vandalism—computers have been bombed, burned and riddled with bullets—to industrial espionage, blackmail and theft.

Moreover, the criminal potential is increased by the ongoing explosion in computer technology and use. So-called "minicomputers," some as small as an office copying machine, are, for the first time, bringing computer technology—and the attendant security problems—to small businesses.

"They (minicomputers) are sitting out in the middle of offices, available to everyone, even the contract janitor," noted Thomas Foster, a computer auditor for the national accounting firm of Main Hurdman & Grant-stoun.

Foster told how one of his client companies was defrauded by an employee who regularly "purchased" goods manufactured by the firm. The worker, a computer operator, never paid for the products, but programmed the computer to "forgive" the amount each month, thus balancing the books.

"The only way that would be caught, would be for someone to go through and manually add up the figures on the computer, but no one would ever do that because everyone assumes computers are always right," Foster said.

The employee was caught when he was absent from work one day and the computer broke down, forcing another worker to man-

ually balance the books, according to Foster.

Many of the elements that make computers attractive to business, industry and government—speed, efficiency and elimination of paperwork—also make them vulnerable to criminal intent. Compounding the problem is the complexity of computer technology and the public's relative inexperience with computer crime.

For example, as recently as four years ago there were no laws in the United States specifically directed toward computer crime, according to Phil Wynn, head of the electronic crimes section of the Los Angeles County district attorney's office. Authorities have prosecuted cases under grand theft, fraud and even forgery statutes, but often it has been like "pounding round pegs into square holes," Wynn said.

Does it constitute grand theft, for instance, to steal a \$50 roll of magnetic tape? Prosecutors would argue that it does when the tape contains a company's computer program the thief might sell to a competitor for \$1,500. A judge unfamiliar with computer processing might disagree, however, "even though that same judge would have no problem saying \$10 worth of paint and \$10 worth of canvas can be valued at \$10,000 if done by a Picasso," noted prosecutor Becker.

Five states have adopted laws defining computer crime and the California Legislature is expected to act this fall on a similar bill by Sen. Lou Cusanovich (R-Woodland Hills).

Don Metzker, the state data processing officer who helped draft Cusanovich's bill, said it tackled the thorny problem of defining as property the electronic signals and commands within a computer program.

Even with a new law, however, most California law enforcement agencies would be ill-equipped to cope with a rise in computer crime, most experts agree.

"Law enforcement is very uninformed about computer security," said former Los Angeles police chief Tom Reddin, now an industrial security consultant. "The people who are best informed are the computer programmers, but they don't think much about security. They just think of all the wonderful things computers can do."

In Orange County, second largest county in the state and the destination for growing numbers of computer-reliant businesses, the district attorney's office admits it is short on expertise when it comes to white-collar crime.

Jack Ryan, who heads the office's fraud unit, said he has no accountants on his staff and thus is dependent on the cooperation of victim businesses, a situation that makes it nearly impossible to penetrate a corporate cover-up.

Relatively few companies are willing to provide that cooperation, Ryan believes. "I'm sure we only see a small percentage of the cases," he said.

Los Angeles prosecutor Wynn agrees. "I think so many times these crimes of allegations are buried and the (suspected) employee is rotated or dismissed," he said. "That's because the companies don't want to wash their dirty linen in public. They don't want the public to know their security has been breached."

But Robert H. Courtney, manager for internal security and privacy for IBM, said it is merely a matter of business sense.

"Often the hurt done by reporting it (in lost public confidence) exceeds the harm done by the crook," Courtney said. "Even if the company does report it, who knows if the prosecutor wants it?"

White-collar crimes are tough to prosecute. It's a lot easier for him (the prosecutor) to go after a bank robber or burglar. He can get four or five convictions a day with those if he's lucky. With white-collar crime, he's got to spend a lot of time and put several investigators

on it to make one case, and even then it's just one more bean on the bean pile."

Courtney also dissents from the view that computer crime is on the rise.

"There's nothing new; these are the same people who have always committed white-collar crime," he said. "What computers may have done is make white-collar crime more democratic."

A greater problem, according to Courtney, is simple ineptitude in computer operations. "The crooks," he said, "are never going to keep up with the incompetents."

In any event, large corporations are paying increased attention to computer security, although they frequently are reluctant to discuss it with outsiders.

It's a matter of survival, according to the computer security chief for a major retail chain.

"Many of our systems are so close to the computer that if for some reason those units went out it would be only a matter of time before we'd go out of business," he said in an interview conducted on the understanding that neither he nor his employer would be identified. "The computer room is looked on as a big bank vault."

Like many large firms, his company decided to train its own computer security specialists from among data processing employees. "We took computer people and taught them security because we found that was a lot easier than taking security people and teaching them computers," he noted.

Smaller companies without extensive data processing staffs do not have the luxury, however. Moreover, one of the reasons they probably bought a computer in the first place was to reduce the number of employees.

If they worry about security at all, executives of small firms are likely to turn for advice to local independent security consultants—usually ex-policemen who know a lot about locks and burglar alarms and almost nothing about computers.

If they do find a consultant who specializes in computer protection, they probably are going to find his advice costly and often unwelcome.

Although most computer specialists believe almost all business computers can be made reasonably secure from tampering, "it's expensive because we're playing catch-up," explained consultant Campbell. In addition, tight computer security also means controls on employees.

"It's extraordinarily difficult when you go into an organization to get people to recognize that the greatest threat is among their own employees," said Peter S. Browne, president of Computer Resources Controls, Inc., a Rockville, Md., security firm where the client list includes Chase Manhattan Bank and the U.S. Dept. of Health, Education and Welfare.

Nonetheless, American Workers today are subject to greater on-the-job surveillance than ever before. More television cameras, metal detectors, magnetic card locks and even lie detectors are finding their way into factories and offices.

Even with sophisticated screening techniques, however, companies might find it difficult to sweep out the potential computer criminal, according to most experts. Parker interviewed 25 computer criminals and found "they're exactly the kind of people a data processing manager would want to hire. They're young, highly motivated, intelligent... They tend to otherwise be highly honest people. They would never steal money from a person."

In any case, security specialists concede they have not kept pace with rapidly changing computer technology.

"It's a catch-up ballgame now," said one. "Many companies are in the position analogous to deciding they have to put a stop sign on a street corner after somebody already has been killed in an accident."

SOPHISTICATED CRIME

(By Angeline Pantages)

It is generally agreed that computer crime is not uncommon, but nobody really knows just how widespread it actually is. The reason is that most crime committed through the manipulation of computers is difficult to detect and, if discovered, is frequently unreported because of the embarrassment to the company involved.

Computer crime expert Don Parker has 670 cases of such abuses in his files at the Stanford Research Institute. They range from the embezzlement of funds to the theft of equipment, from a stock swindle to the destruction of computer centers, from the theft of programs to the stealing of computer time ("Many Ways to Cheat," page 97). Parker readily admits that his files are incomplete. In fact, these cases may represent no more than 5 percent of what is happening, according to security expert Robert Jacobson.

There are many reasons for the failure to detect computer crime, according to Jacobson. A top security director at Chemical Bank who now heads his own New York-based consulting firm. A major one stems from the complexity and capability of techniques to deal with them. Moreover, too many corporations lack good controls and too few auditors assume the responsibility for detecting fraud, maintains Jacobson. The only reason the 1973 Equity Funding swindle was brought to light was that somebody snitched, he points out.

Corporations often are reluctant to report computer crimes because the legal difficulties, the embarrassment and the loss of public confidence can be more damaging to the company than the crime itself. In fact, SRI's Parker readily admits that he advises some of his clients not to report certain computer crimes for these reasons.

Even when computer fraud is reported and prosecuted, convicted computer criminals frequently receive no more than token sentences, particularly if they practiced the "R&R" defense—repent and repay. In many cases, the prosecutors bog down in the complexities of finding and presenting the evidence. A by-product of all this is that computer crime has been bathed in glamour. For some criminals, it represents an intellectual challenge whose rewards include beating the establishment, which can "afford it."

STIFFENING THE LAW

The nation's lawmakers are now attempting to knock the glamour out of computer abuse. The Federal Computer Systems Protection Act of 1979, introduced by Connecticut Senator Abraham Ribicoff and cosponsored by a large bipartisan coalition, would crack down hard on computer crime. The measure, now before the Judiciary Committee, mandates whopping sentences (up to fifteen years) and stiff fines (up to \$50,000) for destruction of computer equipment. For fraud or theft, the bill would fine the culprit two-and-one-half times the amount stolen, in addition to a maximum fifteen-year sentence.

A number of reports from federal agencies show large numbers of computer abuse cases within the government itself. As a result, lawmakers feel the federal communications networks cannot be fully secured and are concerned about massive theft and destruction that could foul up a host of federal programs such as Social Security, veterans benefits and tax collecting. Moreover, the lawmakers are concerned that organized crime is becoming involved in corporate rip-offs and that crucial data could fall into politically "wrong hands."

As electronic funds transfer networks become more commonplace, the nation's banking system is particularly vulnerable to com-

puter crime. And, in the next decade, with most retail customers likely to pay for their purchases through the insertion of a plastic card in a computer terminal, department and other stores are bound to become more susceptible.

A corporation's financial liability for computer crime committed by its employees is a vague, sensitive subject that few care to discuss. Obviously, a company is not automatically open for legal troubles because some programmer pilfers a few million dollars from its coffers. But there are laws and rules that can apply.

Strangely enough, one is the Foreign Corrupt Practices law. Aimed primarily at illegal corporate acts, like bribes overseas, this law also makes management responsible for its accounting and internal controls. Conceivably, corporations could face legal troubles if they are grossly negligent in applying proper data-processing, auditing and accounting controls and as a result suffer in material loss. As better auditing and security appear, the definition of negligence in data processing may be put to the test.

Some federal regulatory agencies are now beginning to issue rules on data processing to the industries they oversee. The Food and Drug Administration, for example, promulgated new regulations last spring that govern how computer systems used in manufacturing, processing, packing and storing drug products should be operated and controlled.

CORPORATE LIABILITY

Lawyer Robert Bigelow, in his publication Computer Law and Tax Report, says that the drug company that fails to "set up and enforce the appropriate controls on security, back up, access, and documentation" may be opening itself to prosecution. And the programmer and systems analyst who fails to do his part may also be liable. Bigelow strongly advises corporate counsel to keep data-processing management up-to-date on such industry regulations.

When it comes to reporting computer crimes, only banks have a legal requirement to do so, lawmakers are often loathe to force business to admit being victims, and that is a major reason so little computer crime has been recorded, according to some experts in the field.

The State of Colorado has just revised its criminal code and has included a statute stating it is the duty of a corporation to report crime, although it isn't a crime not to. Colorado lawmakers say they want to change the attitude toward such reporting and hope companies will view it as a business responsibility.

Not surprisingly, most firms that use computers have policies to protect them from fraud. But the policies generally are not labeled "data processing" and there is no one form to cover everything. That's why Harry Chadwick, senior underwriter at insurance brokers Chubb & Sons Inc., advises companies to seek underwriters who will modify policies to spell out, in plain English, data-processing problems they want covered. While clearer language could mean higher premiums, he advises firms to "pay the price for peace of mind."

"Named peril" insurance can cover damage to equipment by outside terrorists or other criminals, as long as that particular peril is named. "All risk" insurance may also cover such a situation but make sure," says Chadwick.

Other types of policies that should be considered include: employee dishonesty coverage to protect the company from actions by its own workers; business interruption insurance, for those terrible times when the whole system is crippled by destruction of files or equipment; valued paper and other insurance that will cover destructions or theft of specified, valued data.

Since employees are frequently involved in

computer crime, companies should carefully screen applicants for jobs in this area. A corporation's personnel staff, its psychologist and its own sense of ethics and humanity are critical factors in avoiding unnecessary vulnerability. The company should:

- 1. Keep employees happy and fairly treated. The greater the responsibility, the greater the compensation should be.
- 2. Educate employees on security procedures and disciplinary actions for violations.
- 3. Instill a high level of ethics.
- 4. Avoid hiring "high risk" personalities for key jobs.

Distribute key responsibilities in data-processing operations to avoid the "one man knows all" problem.

Track, without violating employee privacy, severe personal problems that may affect business judgment.

Ethics is probably one of the most controversial subjects in the computer field today. A corporation cannot assume uniform standards of ethics among its computer staff. This does not mean data-processing professionals are crooks, but, short of the money and goods, they don't always agree what constitutes a high ethical standard.

Some of this confusion stems from the industry's early history when computer programs were frequently exchanged because of the lack of software. In fact, until recently it was not unusual for programmers at competing service companies to trade software. While such cozy relationships can be perfectly aboveboard, they can contribute to unethical revelations about a competitor.

EXAMINE CHOICES

Another problem is that in the last fifteen or twenty years, university computer science departments have encouraged "computer busting"—finding ways to gain unauthorized access to the system—among the students, often making this practice an assignment. Some academicians defend this as a means of teaching systems design and creativity to students, since they must learn a great deal before they can successfully engage in computer busting.

While this may be true in some instances, students around the nation have been taking advantage of the invitation to be clever. There have been at least half-a-dozen recorded instances in which grades already in a computer have been changed (sometimes for a fee). And recently, at the University of Alberta in Canada, two students were prosecuted for gaining repeated unauthorized access to commercial accounts serviced by university computers. Allegedly, some of their professors had encouraged it.

This case was the focus of a discussion at the recent National Computer Conference in New York. At the session, the industry's professionals demonstrated a wide range of disagreement on whether to teach students to break the system. One professor defended the creative benefits and even denied university responsibility for those who took the assignment too far. "We are not here to teach ethics; they should have learned them before they arrived on campus," he argued.

What can corporations do to protect themselves against computer abuse?

A perusal of the literature and discussions with experts show that self-protection is expensive but necessary. Here's a partial list of do's and don'ts that indicate the difficulties involved:

1. Check corporate liability for failing to apply controls.
2. Analyze the risk of disaster and the potential losses to help determine what preventive steps to take and at what cost.
3. Learn the warning signals that indicate the company may be vulnerable to fraud (for example, a very complex business structure with an effective internal auditing staff).
4. Buy insurance, but make sure the

underwriters know data processing and incorporate your firm's specific requirements in the policy.

5. Make sure that employees understand company ethics and security rules and what will happen if they don't abide by them.

6. Hire data-processing auditors who are of a high caliber and possess a knowledge of computers as well as auditing.

7. Make auditing procedures a part of the computer system design.

8. Audits should be a surprise.

9. Don't use the computer vendor as a primary computer adviser, while loyal and trustworthy, his goal is to sell equipment, not scare you out of it.

10. Use common sense. When it comes to security, watchmen, guard dogs, passwords and padlocks are useless if the back door is unlocked.

While no system is foolproof, a company that employs the do's and don'ts cited is bound to be in a better position to combat computer crime. The cost of not being vigilant could be bankruptcy.

MANY WAYS TO CHEAT

Computers are neither the perpetrators nor the victims of crimes. Computer crime, like all crime, is people-oriented. Someone initiates it; someone benefits from it; someone is victimized by it.

Semantic problems understandably confuse the innocent in any discussion of computer abuse. The computer is a tool, a system separate from the information that is manipulated as the system generates a report, figures a payroll or otherwise performs an assigned task. But often the distinction between the computer and the information becomes confused; the most common of all so-called computer crimes is actually "data diddling"—feeding false or unauthorized information into a computer to produce an inaccurate or phony report.

The computer can, of course, be used as an instrument of crime—usually in planning or testing a scheme. But far more often, the computer system becomes either the environment for a crime (false data input or unauthorized but correct password access, for example) or itself the object of an illegal scheme (in which the system is internally modified to effect a crime).

Categories of criminal computer abuse could probably be created and recreated infinitely. The Federal Deposit Insurance Corp. uses four general categories of threat in discussing the vulnerabilities of data-processing systems: physical, transactional, programming and electronic. Each requires different types of skill, knowledge and access. Physical acts include destructive attacks on equipment, data or programs; false data input through normal manual methods; and scavenging for information available in physical form (printouts, punch cards, disk packs, etc.).

Transactional acts include impersonating (assuming the identity and privilege of another person) and "piggy-backing" (unauthorized second use of a terminal).

Programming acts can include a variety of sophisticated techniques to corrupt the system's controlling software. This is the wonderland for the criminal technocrat, and the next major computer crime may involve an esoteric programming technique called a "logic bomb," or a "Trojan Horse attack." The former is a programmed instruction to a computer to perform an unauthorized act when, for example, the cash balance reaches a certain level. The latter is the placing of an unauthorized program within an authorized one. There are many other techniques in a field still wide open, unfortunately, for intuitive and innovation.

Electronic threats include wire-tapping and computer hardware modifications that could produce the same results as software modifications.

CASE HISTORIES

Since the beginning of the decade, a federally-funded study at the Stanford Research Institute has been collecting and cataloguing case histories of computer-related crime, and the industry trade press regularly reports cases ranging from automated teller belts to extortion. For example, the former employee of a European multinational talked his way into the media library and drove off with a truckload of financial records, tapes and disks, and then stopped to pick up the backup copies at another location before demanding \$1 million ransom.

Some of the more impressive dollar figures are attached to cases in which nothing more sophisticated than false data entry was used. In the Equity Funding case, for example, approximately \$2.1 billion in phony insurance policies were created in the system simply by entering them into the files. After that, it was a matter of using special programs to omit or cover up the bogus policies in billing, balance preparation and other audit statements.

More recently, a Chicago company president, a data-processing manager and a programmer were charged with a \$40 million fraud after allegedly inflating the computerized inventory records to cover up poor management. The hyped inventory was discovered by the board of directors, which in turn set about to deflate the figures slowly to avoid a drop in the firm's publicly traded stock. At this stage, the SEC and Justice Department moved in.

As for physical destruction, computers have been shot, knifed, bombed, battered and had milkshakes poured into them. The perpetrators have been disgruntled employees, dissidents and terrorists. In Italy alone in the last three years, terrorists, with great technological expertise, have blown up 25 computer centers. One of the worst occurrences in the U.S. was the destruction of the Army Research Center at the University of Wisconsin, where one employee was killed.

Automated teller machines have given a computer connection to a lot of old-fashioned con men. Citibank had to modify its auto teller system to require double entry of the magnetic card, at the beginning and end of transactions, because of the "piggy-backing" threat. In a typical case, a customer inserted his card, punched in his password—only to be waved away from the "broken machine" by a man at the bank's emergency telephone. When the cardholder walked away from the teller terminal, a second man rushed over to punch in a withdrawal from the other's account.

Most computer crimes, however, seem to be "inside jobs." The computer system is never more vulnerable than in the hands of those who feed and care for it; and data-processing security is never stronger than the weakest or most vulnerable employee in a position of trust.

The value of unused computer time apparently spurs the entrepreneurial spirit. Two programming managers working for the science and engineering group at Univac's Blue Bell, Pennsylvania, plant were convicted of conspiracy and mail fraud after they used company computers to run a small business arranging sheet music by computer. When they were arrested, their music business was using three-fourths of the computer capacity assigned to the Blue Bell science and engineering group. Elsewhere, there have been several cases of employees at time-sharing firms undercutting their boss' price with their own bid using the boss' equipment.

The possibilities of manipulating a computer's software programs to slip money or information into the wrong hands are numerous. The controller at a chemical firm, aware of the sort of irregularities that alerted auditors to investigate corporate pay-

ments, used the computer to model the company's accounts payable activities so he could issue checks to himself through phony vendor accounts while keeping the cash flow within normal parameters.

One of the now-classic techniques—well understood in theory, but rarely put into effect in real life—is the “trap door.” In the development of large computer programs, programmers usually provide breaks in the code for the insertion of capabilities, for example, subtotals). Most operating systems are designed to prevent additions or modifications to their program code, but programmers sometimes insert these breaks—or “trap doors”—to handle necessary changes while the system is still in development. Although these are supposed to be removed during the final editing of the program, sometimes they are overlooked. There are other cases in which a programmer has built a “trap door” in a program that he could later use for his own, possibly illegal, purposes.

The “trap door” can be used to hide instructions given to the system so that the computer's own internal controls aren't aware of it. It can be like a large well-hidden cave in an otherwise well-patrolled park; anything could be happening in there and no one would know.

A RARE CASE

In one of the rare reported cases, a bright programmer discovered a trap door in a computer system's Fortran compiler and he was able to use it to have the computer execute his instructions secretly. The computer was a commercial time-sharing system and with the trap-door facility this man was able to gain access to the data and programs confidentially filed by other users and have the computer execute large amounts of work without billing him.

Like most ingenious criminal schemes using program techniques, this case was uncovered through an unusual accident rather than through any conventional system-security program. This widespread limitation of security systems is a critical problem in detecting computer crime.

ILLINOIS TAKES THE LEAD IN
COMBATTING COMPUTER CRIME

Mr. PERCY. Mr. President, over the last several years, I have become concerned with the rapid growth of computer crime in the United States. Thus, it was my great pleasure to join with my colleague, Senator RISICOFF, in June 1977 in introducing S. 1766, the Federal Computer Systems Protection Act. This is the first Federal legislation specifically designed to prohibit the misuse of computers owned or controlled by the U.S. Government, financial institutions, or corporations operating in or affecting interstate commerce.

Although that measure did not become law in the 95th Congress, hearings on the bill were held in June 1978 in the Criminal Justice Subcommittee, ably chaired by Senator BIDEN. In the 96th Congress, we have again introduced the measure, now S. 240, with certain re-

visions suggested by the Department of Justice.

We have continued to work closely with Senator BIDEN, and with other members of the Criminal Justice Subcommittee, particularly Senator HATCH and Senator LAXALT. We all want to make certain that S. 240 accurately and effectively reflects the Federal Government's vital interest in stopping computer crime, and in protecting the integrity of the business and financial transactions of this country. I believe we have been successful in that regard. I look forward to early consideration of this measure by the full Judiciary Committee so that the Senate will have the opportunity to take a firm and necessary step in the fight against white collar crime.

The legislation originates from a study released in March 1977 by the Governmental Affairs Committee which revealed the insufficient security of Government computers and the absence of adequate

protection in our Federal laws against computer crime. Prosecutors have found themselves hamstrung trying to fight 20th century crimes with 19th century statutes.

We are moving closer and closer to becoming a cashless society. In so doing, the potential for fraud and abuse through manipulation of computers becomes an ever greater threat. Huge sums of money are already lost each year as a result of computer crimes, with estimates ranging from \$100 million to more than \$3 billion. And the chances of getting caught are minimal.

A few States have begun to take action. I am proud to say that Illinois is among them.

The Illinois State Legislature has recently passed and Governor Thompson has signed a computer crime law. In many of its provisions, it is similar to S. 240. I ask unanimous consent that the text of the Illinois act be printed in the

Rec as following my remarks. The Illinois Legislature is to be congratulated for attempting to combat this problem.

The PRESIDING OFFICER. Without objection, it is so ordered.

(See exhibit 1.)

Mr. PERCY. However, Mr. President, the problem is nationwide, and well beyond the resources and expertise of many State and local jurisdictions. Through the wizardry of electronics, a computer crime can be initiated in California, executed in New York, and affect the lives and assets of people in every State of the Union. It is time that we in the Senate address the national scope of this problem, and move expeditiously to enact S. 240, the Federal Computer Systems Protection Act.

EXHIBIT 1

An Act to add Section 16-9 to and to amend Section 16-1 of the "Criminal Code of 1961", approved July 28, 1961, as amended.

Be it enacted by the People of the State of Illinois, represented in the General Assembly,

Section 1. Section 16-1 of the "Criminal Code of 1961", approved July 28, 1961, as amended, is amended, and Section 16-9 is added thereto, the added and amended Sections to read as follows:

(Ch. 38, par. 15-1)

Sec. 16-1. Property. As used in this Part C, "property" means anything of value. Property includes real estate, money, commercial instruments, admission or transportation tickets, written instruments representing or embodying rights concerning anything of value, labor, or services, or otherwise of value to the owner; things growing on, affixed to, or found on land, or part of or added to any building; electricity, gas and water; birds, animals and fish, which ordinarily are kept in a state of confinement; food and drink; samples, cultures, microorganisms, specimens, records, recordings, documents, blueprints, drawings, maps, and whole or partial copies, descriptions, photographs, computer programs or data, prototypes or models thereof, or any other articles, materials, devices, substances and whole or partial copies, descriptions, photographs, prototypes, or models thereof which constitute, represent, evidence, reflect or record a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention, or improvement.

(Ch. 38, new par. 16-9)

Sec. 16-9. Unlawful use of a computer.

(a) As used in this Part C:

1. "Computer" means an internally programmed, general purpose, digital device capable of automatically accepting data processing data and supplying the results of the operation.

2. "Computer system" means a set of related, connected devices, including a computer and other devices, including but not limited to data input and output and storage devices, data communications links, and computer programs and data, that make the system capable of performing the special purpose data processing tasks for which it is specified.

3. "Computer program" means a series of coded instructions or statements in a form acceptable to a computer, which causes the computer to process data in order to achieve a certain result.

(b) A person commits unlawful use of a computer when he:

1. Knowingly obtains the use of a computer system, or any part thereof, without the consent of the owner (as defined in Section 16-2); or

2. Knowingly alters or destroys computer

programs or data without the consent of the owner (as defined in section 16-2); or

3. Knowingly obtains use of, alters or destroys a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of a computer system (as defined in Section 16-2) or any third party.

(c) Sentence:

1. A person convicted of a violation of subsection (b) (1) or (2) of this Section where the value of the use, alteration, or destruction is \$1,000 or less shall be guilty of a petty offense.

2. A person convicted of a violation of subsections (b) (1) or (2) of this Section where the value of the use, alteration or destruction is more than \$1,000 shall be guilty of a Class A misdemeanor.

3. A person convicted of a violation of subsection (b) (3) of this Section where the value of the money, property or services obtained is \$1,000 or less shall be guilty of a Class A misdemeanor.

4. A person convicted of a violation of subsection (b)(3) of this Section where the value of the money, property or services obtained is more than \$1,000 shall be guilty of a Class 4 felony.

(d) This Section shall neither enlarge nor diminish the rights of parties in civil litigation.

Section 2. This Act takes effect on becoming a law.

Telecommunications Thief Uses Home Computer as a Weapon

By Michael Schrage
Special to The Washington Post

NEW YORK—To the folks at American Telephone & Telegraph Co., Captain Crunch is not just a breakfast cereal. Captain Crunch is the nickname of John Draper, a 35-year-old technical wizard who won notoriety for the skill and ease with which he cracked the Bell System security to place thousands of dollars worth of free calls around the world.

Draper's key to the Bell System was a device known as a "blue box," a multifrequency tone generator that enabled Draper to detect and tap in to Bell customers' WATS lines to make his free phone calls. Luck and months of research were required before the Bell System could track Draper down and amass enough evidence to convict the blue box bandit and send him to prison.

John Draper, alias Captain Crunch, now faces the possibility of going to prison again. Last Monday, in Stroudsburg, Pa., courtroom, Draper pleaded guilty to the charge that he was in "possession of a device used, adapted, or manufactured for the commission of a telecommunications theft."

Yet that device was not an ordinary blue box. When authorities arrested John Draper he had in his possession an Apple II personal computer. The computer, which retails nationally for under \$1,500, was equipped with a telephone interface board that effectively hooked the computer into the phone lines.

Draper insists that the computer hookup was for legitimate purposes, such as automatic redialing, data transmission, and WATS extending.

Ralph A. Matergia, the prosecuting attorney who spent nearly a year preparing for the case, agrees that there was nothing illegal about the computer/home interface but points out that this computer was "programmed to probe for phone lines capable of subversion, search for the access codes to those lines, and illegally place calls through those lines."

Matergia asserts that this is a very important case. "This is the first blue box trial concerning the programming abilities of a computer."

It is also the first reported case of a crime involving the use of a personal computer.

The implications of the case are likely to be far broader than the simple conviction of Captain Crunch. The spectre of computer crime has recently united business and industry alike. Computer crimes on a national scale cost companies an estimated \$100 million annually. And the possibility of computer crimes could be committed by home computer users is a frightening thought to the business community.

Currently, there are an estimated 150,000 home

Chicago Jaycees Quit Over Ban on Women

CHICAGO (AP) — The Chicago Jaycees have withdrawn from the United States Jaycees because the national organization will not admit women members.

The 350-member Chicago chapter severed its national and state ties Wednesday after delegates to the national Jaycees convention in Atlantic City, N.J., voted to keep male-only membership rules.

A proposed by-law change would have allowed state Jaycee organizations to decide whether to allow women as members.

Wednesday's vote in Atlantic City was the second veto of women's membership. The first was at the 1975 convention in Miami.

computers around the country. Industry analysts predict that by the end of five years there will be between 1.5 million and 2 million home computers in use. During that time they are expected to become faster, more powerful and more sophisticated. With that increased sophistication comes the increased possibility that the home computer will be used to commit crimes.

"There's no doubt about it. It's a tool and it can be abused," said Van Chandler, the software manager of Radio Shack's TRS-80, a nationally advertised home computer. "However, the level of sophistication for abuse just isn't there yet."

Radio Shack will be coming out shortly with a telephone interface attachment for its home computer and Chandler concedes that, with modification, a TRS-80 with that accessory could be turned into an ultrasophisticated blue box similar to Draper's.

But Donn Parker, a senior management consultant specializing in computer security at SRI International, a non-profit think tank in Palo Alto, California, is quick to point out that rapidly evolving improvements of home computer technology make the home computer a threat to nearly all businesses with computers, not just the phone company.

"We're certainly starting to look at it as a potential problem," said Parker. "Personal computer crime presents a significant threat to on-line systems, especially to electronic funds transfer."

Parker postulates that a person with a home computer who can obtain access to a corporate computer system could conceivably subvert and exploit the system for his own benefit.

"The personal computer is more of a threat to such a system than an ordinary computer terminal," Parker said. "The personal computer gives the user a greater amount of leverage."

Rather than place restrictions on home computer technology, Parker calls for developing new and more powerful computer security systems and implementation of data encryption techniques.

Yet the versatility of the home computer is not limited to dealing with other computers. Parker mentions that the home computer could be programmed to simulate or model various situations and events to practice committing a crime.

Moreover, the computer's inherent strengths lend itself to the commission of complex and intricate crimes. Parker relates the story of a London, England, check-kiting scheme of 1975. The game had amassed thousands of pounds illegally by taking advantage of the float between deposits and withdrawals at various banks. The gang had a minicomputer monitor the various transactions to assure that no deposits or withdrawals would be mistimed.

Unfortunately for the criminals, the computer they used malfunctioned, their scheme collapsed, and they were all arrested. While a home computer was not involved in the commission of this crime, Parker asserts that, with proper programming, a home computer could easily have been used.

Of course, computers have had less glamorous partnerships in crime. One computer store owner ruefully tells the story of how she sold a computer to a suspicious looking man who later was arrested for fencing stolen property. His home computer was used to keep track of his inventory.

In an effort to deal with the rising problem of computer crime the Senate Subcommittee on Criminal Law is hearing testimony this week on Senate Bill 1766, the Federal Computer Systems Protection Act.

The act is an omnibus proposal that would outlaw unauthorized use of computers and computer resources. Observers say that the breadth and scope of the bill should discourage those who would commit home computer crimes. It is also felt that the rapid proliferation of home computers has lent a sense of urgency to revise the law to deal with their abuse.

PERSPECTIVE

Curbing Fraudulent Computer Usage

By Sen. Joseph R. Biden, Jr.

Within the whole spectrum of contemporary concern with public corruption and fraud, no problem has proved to be more acute or resistant to solution than the fraudulent or illegal use of the modern electronic computer and computer systems.

Current federal criminal statutes do not adequately cover computer fraud and abuse. Federal prosecutions of computer crime have had to be pursued under a variety of mail and wire fraud statutes, some of them dating back to the 19th Century. As might be expected, these aging statutes have fallen woefully short of dealing with the most modern of crimes.

The Senate Judiciary Subcommittee on Criminal Justice has been acutely aware of the law's shortcomings with regard to computer fraud, and after extensive research, the subcommittee is prepared to do something about it — by agreeing unanimously to report the Computer Systems Protection Act of 1979 (S. 240) for consideration by the full Senate Judiciary Committee.

Computer-related crime was brought to the attention of Congress by a Government Accounting Office study in 1976. The next year, the Senate Governmental Affairs Committee reported on "Computer Security in Federal Programs." In 1978, the Criminal Justice Subcommittee held two days of hearings. The studies and the testimony made it clear that computers are vulnerable to unauthorized and illegal access, that computers are often not adequately screened and supervised, and that, as we have seen, federal statutes do not adequately cover computer crime.

In this Congress, analysis of the legislation has focused on three principal areas: (1) defining terms that seemed vague and confusing, both to persons charged with enforcing the law and to individuals who work with computers; (2) deciding which offenses should be included and what would be the appropriate sanctions, and (3) defining the scope of federal jurisdiction more specifically.

Bill S. 240 now makes it a crime — punishable by up to five years in prison and a fine of up to twice the illegal gain, or \$50,000 — to use a computer to steal or to execute a fraud.

A person who commits a traditional

theft or fraud will no longer escape prosecution merely because he uses an untraditional device — the computer — to perpetrate the crime, and the magnitude of the potential fine should deter those willing to risk prosecution in hopes of obtaining tremendous gain.

The bill also makes it an offense — subject to the same prison term and a fine of up to \$50,000 — to damage a computer. This provision is aimed at damage to a computer or its assets by terrorists, disgruntled employees or anyone who intentionally, and without authorization, damages a computer.

The broad definitions of the terms "computer," "property" and "use" required by the continuing rapid development of computer technology are contained in the bill. The definition of "computer" has been narrowed, however, to exclude such things as automated typewriters and typesetters, and personal computers, including hand-held electronic calculators. Mere "access" would not be an offense under the bill, unless the access amounted to a theft of the computer's services.

The broad definitions in the bill are offset by specific limitations on the scope and exercise of federal jurisdiction, which would apply only to computers operated by the U.S. government or financial institutions and to computers operating in, or over facilities operating in, interstate commerce.

The subcommittee recognizes that most computer crimes should be prosecuted by the states, and a number of states have computer-crime legislation already on the books or in process now.

Passage of the Computer Systems Protection Act will give federal law enforcement an important tool in combatting computer-related crime. It should also deter potential offenders and encourage the reporting of computer crimes.

But this legislation, important as it is, is merely a first step toward effective control of computer-related crime. Needed most, and yet to come, are measures to more surely protect the security of data processing systems — measures which, for the most part, must be taken by industry, the producers and the users of computer systems.

Joseph R. Biden Jr. is a U.S. senator from Delaware and chairman of the Senate Judiciary Subcommittee on Criminal Justice.

S. 240 - Computer Fraud & Trial of Stanley Rifkin

The Computer Fraud and Abuse statute, as proposed, goes to the heart of activities like those discussed in the newspaper account you enclosed. While the initial perpetration, as described, does not appear to have required a complex assault on the computer system or its programs, it apparently necessitated a thorough understanding of the integration of the computer into banking procedures. It is clearly within the ambit of S. 240 as drafted, though it might well be classified as a wire fraud or banking violation.

It is useful to note that Rifkin had also been alleged to be involved in a second crime, an attempt to steal \$50 million in the transfer of funds from the Union Bank of Los Angeles to the Bank of America in San Francisco. The Government did not go forward with this case against Rifkin. Nonetheless, the Justice Department's comments on this second Rifkin matter are of interest. Mr. Heymann wrote:

Alternatively, the subsequent activities described, since purportedly perpetrated within a single state might have failed the jurisdictional requirements of wire fraud or other existing Federal proscriptions, and be assailable only by a statute such as S. 240, if enacted.

Mr. President, I request that my letter of February 14, 1979, to Attorney General Griffin Bell; Mr. Heymann's March 26, 1979, reply; and a Wall Street Journal article of February 14, 1979, be printed in the RECORD.

The material is as follows:

FEBRUARY 14, 1979.

HON. GRIFFIN BELL,
Attorney General,
Department of Justice,
Washington, D.C.

DEAR MR. ATTORNEY GENERAL: The enclosed article from the February 14, 1979 Wall Street Journal concerns the government's cases against Stanley Mark Rifkin, the computer consultant who is alleged to have stolen \$10.2 million from the Security Pacific Bank in Los Angeles and is alleged to have fraudulently transferred \$50 million from the Union Bank of Los Angeles to the Bank of America in San Francisco.

The Rifkin cases are of interest to me because of S. 240, the Federal Computer Systems Protection Act. According to this Journal article it would appear that Mr. Rifkin's alleged actions in these cases involve the indirect access to computers of financial institutions in furtherance of a scheme to defraud. These cases are the kind I had in mind when I drafted S. 240. Would you be kind enough to let me know if S. 240, as introduced January 25, 1979, would be actionable in the Rifkin cases? In addition, I would like to know if the government is in any way handicapped in the Rifkin cases because there is no federal computer crime statute as envisioned in S. 240.

Your assistance in this matter is very much appreciated.

Sincerely,

ABE RIBICOFF.

U.S. DEPARTMENT OF JUSTICE,
Washington, D.C. March 20, 1979.

HON. ABRAHAM RIBICOFF,
Chairman,
Committee on Governmental Affairs,
U.S. Senate, Washington, D.C.

DEAR MR. CHAIRMAN: This is in response to your letter of February 14, 1979, inquiring into the applicability of S. 240 in the Rifkin case. While I cannot discuss the merits of

the particular case, I will be glad to address your questions in a general sense.

The Computer Fraud and Abuse statute, as proposed, goes to the heart of activities like those discussed in the newspaper account you enclosed. While the initial perpetration, as described, does not appear to have required a complex assault on the computer system or its programs, it apparently necessitated a thorough understanding of the integration of the computer into banking procedures. It is clearly within the ambit of S. 240 as drafted, though it might well be classified as a wire fraud or banking violation.

Alternatively, the subsequent activities described, since purportedly perpetrated within a single state, might have failed the jurisdictional requirements of wire fraud or other existing Federal proscriptions, and be assailable only by a statute such as S. 240, if enacted.

I trust that this response, although belated, is helpful. As you can appreciate, only the prosecutor who investigates and ultimately understands all the aspects of a case can most effectively determine the appropriateness of charging specific violations.

We have discussed S. 240 on the phone recently and should you have further questions, I would be pleased to hear from you. Very truly yours,

PHILIP B. HEYMAN,
Assistant Attorney General.

[From the Wall Street Journal, Feb. 14, 1979]
DEPENDANT IN A PLOT TO TRANSFER MONEY
FACES NEW CHARGES

LOS ANGELES.—Stanley Mark Rifkin, who allegedly stole \$10.2 million from Security Pacific Bank here in October using a complex wire-transfer scheme, is being accused of again attempting to transfer money fraudulently.

The U.S. attorney's office here charged that the 32-year-old computer consultant, along with a friend, Patricia Ferguson, attempted last Monday to transfer \$50 million from Union Bank here to the Bank of America in San Francisco.

Mr. Rifkin had been free on bail in the Security Bank affair, awaiting the start of his trial tomorrow. But while free, he apparently hatched another money-transfer scheme with Miss Ferguson that eventually involved an undercover Federal Bureau of Investigation agent, according to an affidavit by the agent filed in federal court here yesterday.

The affidavit filed by the U.S. attorney's office stated that Miss Ferguson, who had mortgaged her house to help post Mr. Rifkin's original bail, met with the undercover FBI agent last Friday. The U.S. attorney's office declined to elaborate yesterday on the agent's affidavit or to say who initiated the contact.

According to the agent's affidavit, Miss Ferguson allegedly requested that the undercover agent contact an unidentified "banker" at Union Bank about making a fraudulent wire transfer. On Monday, Mr. Rifkin allegedly met with the agent to tell him how to accomplish the wire transfer.

Mr. Rifkin told the agent he planned to use the transferred money to purchase bearer bonds in San Francisco and then immediately leave California, the affidavit alleges. According to the agent, Mr. Rifkin said he planned to make the transfer "pretty much the same way" as he had at Security Pacific, but this time to do it right.

In the Security Pacific affair, Mr. Rifkin was caught by the FBI in San Diego two weeks after the alleged \$10.2 million theft had taken place. In that two weeks, Mr. Rifkin had flown to Switzerland and purchased \$8.1 million in diamonds that he apparently planned to sell upon his return to the U.S.

S. 240 AND THE RIFKIN CASE

● Mr. RIBICOFF, Mr. President, as the author of the Federal Computer Systems Protection Act, S. 240, I was interested in the trial of Stanley Mark Rifkin, the computer analyst who was convicted and sentenced to an 8-year term in connection with the theft of \$10.2 million from the Security Pacific Bank of Los Angeles. I asked the Department of Justice if S. 240 would be actionable in the Rifkin case. Philip B. Heymann, Assistant Attorney General, Criminal Division, replied for the Department and said:

In a pretrial ruling last week, a federal judge held that key evidence in the government's case against Mr. Rifkin, including the diamonds, was "inadmissible as evidence." The judge said that the arrest warrant for Mr. Rifkin didn't provide the proper source material and that therefore the arrest by FBI agents in San Diego, was a case of "illegal search and seizure."

Last Monday, the U.S. attorney's office decided against appealing the judge's ruling, citing the "negative impact of delaying the case."

Both Mr. Rifkin and Miss Ferguson were arrested yesterday after the U.S. attorney's complaint against them was filed in federal court here. A magistrate set the bail for each of them at \$1 million.

The complaint charged both Mr. Rifkin and Miss Ferguson with "conspiring" to "cause false entries to be made" in a bank money-transfer system.

In the Security Pacific scheme, the bank said earlier that Mr. Rifkin gained access to the bank's wire-transfer room last Oct. 25 because bank personnel recognized him as a consultant to one of the bank's contractors. While inside, Mr. Rifkin observed that day's security coding, according to a bank spokesman.

Later that day, Mr. Rifkin, impersonating a bank officer, allegedly placed a call transferring the \$102 million to a New York City bank. He then withdrew the money from the New York bank and flew to Switzerland, according to federal authorities.

A Union Bank spokesman said last night that he hadn't any knowledge of the alleged scheme by Mr. Rifkin and Miss Ferguson. ■

HALT FRAUD AND ABUSE FROM EXCESS MEDICARE PAYMENTS FOR BLOOD AND BLOOD PRODUCTS

● Mr. PERCY, Mr. President, the Federal Government must respond swiftly whenever abuses of our Nation's health care programs are uncovered. Otherwise, escalating health care costs will be fueled at a rate that not only drains the taxpayer's resources but also undermines our Nation's health.

On February 26, 1979, the U.S. General Accounting Office released a report which found that certain independent blood banks have disregarded medicare billing instructions resulting in a multi-million-dollar annual abuse of medicare funds. Mr. President, I shall submit for the Record selected highlights of the report.

The GAO first notified the Health Care Financing Administration (HCFA) by letter on December 12, 1977, that improper blood charges and payments were being made. However, HCFA has yet to revise its regulations or institute corrective actions to eliminate these costly abuses. I am concerned that HCFA respond immediately, before more taxpayer funds are misapplied. To this end, in a letter dated March 22, 1979, I requested a detailed report from HCFA describing:

First, the present steps being undertaken to correct the abuses, and
Second, efforts that have been made to detect and recoup improper medicare payments to blood banks.

Mr. President, I shall submit for the Record a copy of the letter.

I must emphasize, Mr. President, that GAO's investigative efforts on this issue have been exemplary. When the Federal Government receives such thorough docu-

mentation demonstrating abuses of its program, the affected Federal agencies must respond promptly. I trust and expect that Assistant Secretary for Health Dr. Julius Richmond will take prompt action in this regard, consistent with the high priority President Carter and HEW Secretary Joseph Califano have both assigned to the elimination of blatant fraud and abuse involving precious taxpayer moneys. I am awaiting Dr. Richmond's response.

The material submitted follows:

U.S. SENATE,
Washington, D.C., March 22, 1979.
Hon. JULIUS RICHMOND,
Assistant Secretary for Health, Department
of Health, Education, and Welfare,
Washington, D.C.

DEAR DR. RICHMOND: On February 26, 1979, the General Accounting Office issued a report entitled, "Actions Needed to Stop Excess Medicare Payments for Blood and Blood Products." As the ranking minority member of the Permanent Subcommittee on Investigations, with direct oversight responsibility for HEW health care programs, I have given close attention to the GAO report and view its findings with considerable concern.

The GAO report notes that blood banks typically charge a "processing fee" which covers the cost to process a unit of blood. Other blood banks charge an additional "nonreplacement fee" which is assessed when a patient may enroll in a blood insurance program to compensate for these nonreplacement fees, a patient may enroll in a blood insurance program. Such a program guarantees replacement of blood used by its members.

Presently, Medicare pays all blood processing fees. Medicare will also pay nonreplacement fees beyond the first three units of blood used. However, if a patient is enrolled in an insurance program or is able to find the necessary donors to replace blood used, Medicare is not obligated to pay the nonreplacement fee. (Section 3235.B of the Health Insurance Manual—15, Section 2103 of the Health Insurance Manual—16)

The GAO findings show that for the past several years the blood banks investigated have prevented Medicare patients from replacing the blood when it was available through blood insurance programs. Instead, these blood banks chose to bill Medicare for nonreplacement fees—opting for money over blood at considerable expense to the federal government.

The GAO estimates that these overpayments could total millions of dollars annually. In these times of escalating health costs, the Medicare programs cannot tolerate such abuse. Affordable blood and blood products are essential elements of our national health. We must reduce these unwarranted costs to the taxpayer.

The GAO report notes that disparate treatment of Medicare and non-Medicare patients by some community and hospital blood banks is a prime factor contributing to the overpayments problem. In spite of HEW regulations emphasizing equal treatment of both Medicare and non-Medicare patients, GAO found:

"... The blood banks we visited did not treat Medicare patients the same as non-Medicare patients for reducing or eliminating blood fees. The blood banks limited the number of blood credits they would release to offset nonreplacement fees for Medicare patients but placed no such limitations on non-Medicare patients. Some blood banks also allowed credits for non-Medicare patients for either component or blood processing fees but did not allow such credits for Medicare patients." (GAO Report, p. 5)

With respect to the unequal treatment of Medicare patients, then-Health Care Finance Administrator Robert Derzon com-

mented on February 1, 1978, that both Medicare and non-Medicare beneficiaries must be treated equally in any situation regarding blood. Nevertheless, Administrator Derzon stated that the resulting effect of unequal treatment of Medicare and non-Medicare patients has been to:

"... a disproportionately increase Medicare's share of the cost of blood where a provider accepts blood replacement from non-Medicare beneficiaries but not from Medicare beneficiaries. Similarly, to reject replacement credits for Medicare beneficiaries where such credits would reduce blood processing costs or blood component fees is neither a consistent nor a prudent and cost-conscious practice on the part of a provider."

(GAO report, p. 48, Appendix IV, Comments to Question 1.) (emphasis added)

Clearly, the intent of HEW regulations governing Medicare payments for blood and blood products is now being subverted on a national scale by certain community and hospital blood banks. These Medicare overpayments abuses were brought to the attention of HCFA officials by GAO during December, 1977. Yet during the intervening 14 months, it appears that no corrective actions have been instituted.

Unfortunately, as the GAO notes, present HEW regulations governing Medicare payments for blood and blood products are inadequate to alleviate the abuses identified in its report. In light of Secretary Califano's own noteworthy and progressive efforts to curb mismanagement and eliminate the \$7 billion worth of fraud in HEW programs, the GAO's proposals to tighten HEW regulations and recoup past Medicare overpayments assume a particular urgency. Whatever the legal considerations may be in recouping past overpayments, a serious effort must now be made to return these monies to the federal government.

Moreover, I remain unconvinced that remedial legislation—as proposed by HEW Inspector General Morris, to broaden HEW enforcement against suspect blood bank practices—is needed to solve what is essentially an internal administrative problem. (See GAO report, p. 30, Appendix II, Overview) Congress need not pass new legislation whenever a deficiency in program management develops, as in this instance involving fraudulent practices by some community and hospital blood banks. HEW should act—now; it need not wait for Congress to force it to do something—eliminate fraud—which it should do without being told and which the American public has every right to expect it to do.

I therefore request forthwith a detailed report describing:

Present steps being undertaken by HEW to correct the Medicare overpayments problem as discussed in the GAO report. This should include, but not be limited to, a specific timetable for implementing revised regulations; HEW efforts to detect and recoup past Medicare overpayments resulting from improper hospital and community blood practices.

Your attention to this matter is greatly appreciated. If you have any questions, please have one of your staff members contact Chuck Berk, Special Counsel to the Senate Permanent Subcommittee on Investigations, at 224-1117.

Sincerely,
CHARLES H. PERCY,
Ranking Minority Member.

[Comptroller General's report to the Congress]

ACTIONS NEEDED TO STOP EXCESS MEDICARE PAYMENTS FOR BLOOD AND BLOOD PRODUCTS

DIGEST

Medicare insurance for the aged and disabled covers health care services, including blood-and blood products. It reimburses hos-

The Electronic Criminal

How and why computer crime pays

Recently, a gang of European criminals, including a bank executive, stole \$900,000 by simply running a float fraud between two banks for several years. Deposit records were altered in the banks' data-processing centers so cash deposits would appear when there none; the felons then withdrew cash.

In London, a 15-year-old school-boy, not to be outdone by his "elders," cracked the security system of a major computer time-sharing service, gaining access to secret files and changing them at will.

And, not to be surpassed by "foreigners," a major bookmaker in a large midwestern state used unauthorized time on a local university's computer system to calculate his "handicaps."

The above cases are only a few of the more sensational examples which illustrate an increasingly serious problem for law enforcement officials and the American public—the electronic criminal in the computer age. There are today more than 100,000 privately-owned computers in use in this country. The federal government alone operates more than 8,000. The United States Chamber of Commerce estimates that computer crime costs the American taxpayer more than \$100 million each year. This does not even include the cost of security. A recent study by the General Accounting Office revealed that computers are inadequately protected against vandalism, terrorism and program manipulations.

Computers lend themselves to

attack and manipulation largely because our criminal justice system lags so far behind in confronting the problem of computer-related crime—and white-collar crime in general. Experts estimate that the chance of an electronic crime being uncovered is one out of a hundred. To date, no police agency has discovered a major computer fraud. Law enforcement agencies are, for the most part, inadequately trained to deal with such crimes; they must rely on chance discoveries or on insiders who "blow the whistle."

And even when computer crimes are discovered, the number of criminals who are caught and actually prosecuted is very low. Little wonder, then, that the head of the Illinois Bureau of Investigation has warned that organized crime is beginning to show great interest in this new market.

The time has come when new legislation is needed to take technology into account. We need to educate police and prosecutors to the special demands of a computer age.

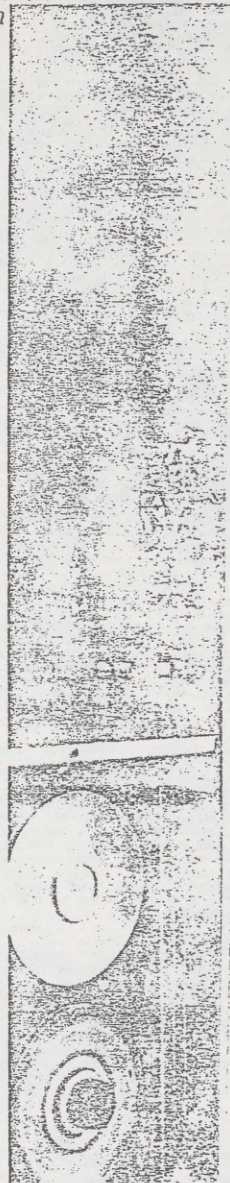
To understand the need for such special efforts, it is worth looking at why computer crime does pay—and pay well.

Thefts by computers usually fall into one or more of the following categories: financial thefts, property thefts, thefts of data, thefts of services and sabotage. These types of crimes not only differ in their *modus operandi*, but also in the sophistication and caliber of the criminals involved in their perpetration.

Computer frauds involving finan-

By August Bequai

Attorney, Washington, D.C. and Consultant to
Congress on Science and Technology



Special Pre-Publication Offer

REQUIRED READING

"DEBTORS' AND CREDITORS' RIGHTS AND REMEDIES" (1975 Revised Edition)

by Sidney Sherwin, Esq.

*Member of the N.Y. Bar; Counsel to the
Profession in Debtor-Creditor Relations*

PART I: DEBTOR'S RIGHTS & REMEDIES

includes these chapters:

Property exempt from execution, "straight" bankruptcy (questions asked by referee), the wage earner's plan, composition agreements, assignment for creditors (when used & procedure), Chapt. XI & Chapt. X Bankruptcy proceedings (when & how used), other statutes for debtor relief (when & how used), "unconscionable" contracts.

PART II: CREDITOR'S RIGHTS & REMEDIES

includes these chapters:

How to locate a "skip", laws of libel, extortion, postal regulations, collection devices, how and when to use each, enforcement proceedings, how to protect creditor in bankruptcy.

STEP BY STEP STAGES, complete with forms from the author's actual case files.

By Sidney Sherwin and already in print. \$19.95

"HOW TO COLLECT A MONEY JUDGMENT"

A "bread & butter" book for every attorney.

The invaluable contents include:

Trade secrets for the collection of "skips", how to find "hidden" assets (without wasteful subpoenas or enforcement proceedings); what to do about fraudulent transfers; how to locate debtor's bank accounts. A practical approach to the use of the law to collect your money judgment.

Over 100 pages of forms and letters used in actual cases.

Hard Cover \$22.00

**Send Coupon Below
TODAY!
PRE-PUBLICATION OFFER**

Attorney's Aid Publications, Dept. AB
P.O. Box 239
Kew Gardens, N.Y. 11415

If you order BOTH BOOKS now, enclosing check for \$32.50 (regularly \$42.45) we will send you HOW TO COLLECT A MONEY JUDGMENT now, and later send you DEBTORS' AND CREDITORS' RIGHTS & REMEDIES (regularly \$19.95).

I enclose \$22.50. Just send HOW TO COLLECT A MONEY JUDGMENT.

I enclose \$19.95. Just send DEBTORS' & CREDITORS' RIGHTS & REMEDIES. You will pay mailing costs.

NAME _____
ADDRESS _____
CITY _____ STATE _____ (ZIP) _____

ces may take any of several forms. This type of crime involves a computer system used for financial processing work such as payrolls, accounts payable and receivable, and the storage of data.

THE CATEGORIES AND SCOPE OF COMPUTER CRIME

Thefts of property by computer often involve stealing merchandise for resale, or even personal use. Four years ago a group of criminals, by manipulating the Penn Central Railroad's computer, diverted more than 200 freight cars to a small railroad in Illinois. In another case, a group of electronic criminals placed orders with a company's computer for various electronic equipment and then sold this material to others. Before they were finally apprehended, they stole more than \$1 million worth of property. The ringleader was put on probation.

Thefts of data and of services usually involve unauthorized access to the computer system, either via remote terminals or when the system is insufficiently protected.

For example, in one instance, a California computer programmer who fell behind in his gambling debts to organize crime was forced to make available confidential programs to these criminals.

In another case, employees of a large mail-order firm stole and sold to a competitor the "most valued" customer list of their company. The estimated value of the list was close to \$3 million. The company never pressed criminal charges for fear of public embarrassment.

Financial reward is not always the sole motivating factor behind computer-related theft, nor are professional criminals or white-collar workers alone in attempting such activities.

Recently, a group of schoolboys cracked the security system of a major computer time-sharing service and gained access to its most secret files. Not to be outdone, another group of students gained access to the computer system at a large university and changed the grades that their professors had stored in it.

Thefts of services involving computers are very common. A politician running for office in a major city was found using that

city's computer for mailings to his district. In another recent case, a very efficient "blackmailer" browsed through computerized credit reports to locate victims who were "loaded."

The final and most serious form of computer crime is sabotage. This usually involves intentional damage to the system. Such attacks may come from domestic or foreign elements. They may come from disgruntled employees or agents of foreign powers. Several years ago the Pentagon's computer system was bombed, making it inoperable for 29 hours. A top security computer system was also bombed at a midwestern university. The damages totaled more than \$15 million. In St. Louis, a suspicious fire at the U.S. Army center destroyed more than 16.5 million personnel records.

WHY COMPUTERS ARE SO EASY TO ATTACK

To understand why the computer proves a tempting target for the white-collar criminal, it's necessary to look first at the system itself. Basically, a computer operation consists of five easy steps, and although computers grow in sophistication and storage capacity, these key steps remain the touchstones of the system.

The first step to any computer operation is the "input"—the point at which data is translated into a language that the computer understands. At this stage, the criminal might introduce false records or alter current ones by removing key input documents. A few years ago five individuals, including the vice-president of a major New York bank and the branch manager of another, stole more than \$500,000 by running a float fraud between the two banks. For four years, deposit records were altered in the banks' data-processing centers so as to appear as cash deposits; the men would then withdraw cash. The fraud was detected only after a bank messenger failed to deliver some checks for a fraudulent "cash" deposit, and they overdraw one of their accounts by \$440,000.

In the second, or "programming" phase, a computer is provided with step-by-step instructions for solving problems. Any criminal with a basic understanding of computers

can easily alter, delete or destroy a program at this stage.

In fact, the first federal criminal case involving a computer occurred in 1966 when a young programmer, faced with financial problems, put a "patch" on his program so that his checking account would be bypassed as the computer checked for overdrafts. Three months later the patch was still in the program and he was \$1,300 overdrawn. The crime was discovered only after the computer happened to break down, and hand calculations revealed the discrepancy.

Programs also lend themselves to "kidnapping" schemes. For example, one young programmer took all the programs of his employer, a medical accounting firm, then went to hide in the mountains and told his employer he wanted \$100,000 to return the "hostages."

"Thefts of programs are common," one witness told a shocked court in a recent case. He should have added that prosecutions are extremely rare.

The third key step to a computer operation involves the CPU or "Central Processing Unit." This is the computer's brain and is vital to the system. The CPU responds to the many problems the computer faces, based on instructions it receives from the program. However, it is extremely vulnerable to attack from wiretapping, electromagnetic pickups or browsing.

Several years ago a programmer, by tapping into a CPU, made away with valuable trade secrets. The authorities issued a warrant to search the memory of the computer for evidence. The programmer was finally convicted, but given a suspended sentence.

The "output" is the fourth step in the process. Here, data passed on from the CPU is translated into a language that is intelligible to the user. It is at this stage that mailing lists, payment records and other valuable data are open to alteration and theft.

With such thefts occurring more and more, the threats—for business in terms of valuable data being sold to competitors or for governments, in instances which might involve military secrets being sold to a foreign power—become increasingly probable.

The "communication" step is the final phase of the operation, when data is transmitted back and forth between computers or between computers and remote terminals. This usually involves use of telephone or teleprinter circuits. Criminals can gain access through various means of electronic interception to alter, modify or even copy data. Part of what makes discovery of such thefts or manipulations so difficult is that the criminal can be thousands of miles away when the actual crime occurs and, as a result, even if a criminal's identity is

known, apprehension is made especially difficult because few laws regarding theft or fraud can be applied to such circumstances.

THE HOPELESS INADEQUACY OF OUR CURRENT LAWS

To deter criminals from attacking a computer system, the prosecutor needs an adequate arsenal of laws to bring offenders to justice. Certainly the current statutes are defective when dealing with the electronic criminal.

The "mail fraud statutes" presently pose the most formidable weaponry in the prosecutor's arsenal, but these laws deal with offenses involving the Postal Service of the United States. There is little likelihood that the computer criminal will use the mails.

The bank statutes provide up to five years imprisonment and up to \$5,000 in fines for anyone involved in the embezzlement or theft of "funds" from federally-insured banks, but these statutes are inadequate for several reasons.

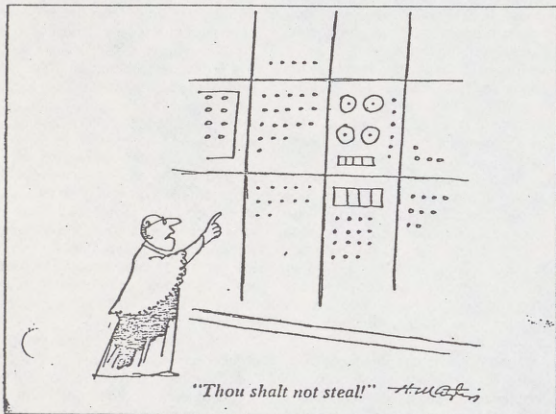
First, non-federally-insured banks are excluded.

Second, the statutes cover only "insiders." The offender must be either an employee, officer or agent of the bank. Thus, a bank which is victimized by a criminal penetrating the system from outside would not be covered.

And finally, the statute provides for the unlawful "taking or concealing of funds." If such a term is to be applicable to transactions involving a computerized system, we may need to redefine the term "funds." What relevance does the concept of paper money have to a system that transfers funds electronically?

Title III of the Omnibus Crime Control and Safe Streets Act makes it a federal crime to willfully intercept any wire or oral communications. Again, there may be problems in terms of applicability. The act had as its objective the protection of private oral or wire communications; it was never intended to protect financial institutions. Furthermore, transmittals involving a computer system may be coded, but certainly they will not be oral. Furthermore, federal counterfeiting and forgery statutes have little effect

(Please turn to page 30)



Electronic Criminal

(Continued from page 11)

in deterring a computer criminal. Breaking a systems code will not fall under these laws.

At present the most effective law has proven to be Title 18 of the United States Code, Section 1343, which makes it a crime to use "wire, radio or television" communications in interstate commerce for illegal purposes. Recently, the United States Attorney's Office in Maryland prosecuted a computer felon with the aid of this statute. The federal prosecutors did note, however, that although this case involved one of the simpler forms of computer crime, prosecution was not easy because the jury had a difficult time understanding what the experts were saying. In other words, at present, computer criminals can rest at ease: few laws on the books cover their activities, even in part.

BRINGING COMPUTER CRIMINALS TO THE COURTS

Prosecutors rely mainly on investigatory agencies to bring computer crime cases to their attention. At the federal level, this work is done by such specialized agencies as the Securities and Exchange Commission or the Federal Bureau of Investigation. However, as U.S. Senate investigators were surprised to learn, no civilian agency has—or ever has had—a trained cadre to investigate computer frauds. In fact, federal investigators are given no such training save in a very peripheral manner.

Things fare no better at the local level. State and city prosecutors rely on local police forces to investigate and detect computer crimes. At present there are more than 17,000 police agencies in this country, but more than 50 percent of these have fewer than 10 full-time employees on their payrolls. Fewer than 50 percent meet the minimum requirements to deal effectively with traditional and unsophisticated forms of crime; none has the capability to handle computer frauds. As one high-placed police official recently confided, "we're in trouble in this area."

Even after a case is brought to the attention of the prosecutor, difficul-

ties continue. Aside from the problems juries have in dealing with experts' detailed testimony about computers, our present rules of evidence make it difficult to introduce computer-generated evidence into a trial. Computer reels or printouts fall under the "hearsay rule" as evidence of a written statement made out of court. To introduce such materials in court as proof of a fraud, they must be brought in under one of the exceptions to the rule. For example, under common law, regular business entries were introduced under the "shop book rule" exception.

The objective of this exception is to allow into evidence only reliable business records. However, to fall under the "shop book rule" or business records exception, a record must have been entered: (1) as a routine part of regular business; (2) within a reasonable period of time after a transaction is recorded, but preferably contemporaneously; (3) by an individual who is not available as a witness; (4) by someone who had knowledge of the event transcribed, and (5) by someone who had no motive to misstate.

Computer-generated evidence, however, is difficult to bring in under this business records exception because it is not usually entered routinely as a regular course of business; it is not entered contemporaneously and, even if it were, it may have been entered into the computer banks by a number of individuals, none of whom had any personal knowledge of the event.

A further difficulty is the reluctance which courts have shown to allow computer-generated evidence into a trial. Cases involving such evidence have been few and usually have been settled out of court.

The Supreme Court recently turned down, without comment, an opportunity to specify standards for using computer-generated evidence at a trial. The justices had been asked by a company seeking to overturn a \$7 million judgment in a breach of contract case to decide whether the main evidence against the company at the trial should have been ruled inadmissible in view of

the fact that the evidence was generated by a computer. The Court ruled that the company could not inspect the computer program used in obtaining the evidence.

There are also serious constitutional questions, such as whether the admission of computer evidence violates the confrontation or due process clause. But these questions will be for the courts to decide over a period of time, and before that can occur we will need to define our legal concept of what constitutes crime in this new, electronic age.

Except in cases of sabotage, computer-related offenses are not acts of violence. There are no smoking guns, blood-stained knives or wailing police sirens. In most cases they are "white-collar crimes," and as a legal concept they have no significance, nor are they found in our criminal codes or statutes.

The cost of avoiding this issue—as the cases I have related show—can be measured in more than dollars and cents. That is substantial enough, but even more dangerous is the widespread effect they have had in terms of the loss of public confidence in the integrity of our political, economic and governmental institutions. Corruption at all levels of government is being uncovered with alarming regularity.

In industry, disclosures over the past two or three years indicate that some of the nation's most prestigious firms have routinely engaged in either illegal or questionable business practices. Corporate looting and manipulations threaten not only stockholders and creditors, but the public as well. They are now becoming commonplace in the colleges and universities, which are our centers of training.

The problem, however, is not so much with computer technology as it is with the inability of the legal structure to adapt and prove flexible in a world where technology is an everpresent reality. As lawyers, we should pause and ask ourselves how long we can afford the luxury of moving at a snail's pace. The electronic criminal poses a challenge. It is time to meet that challenge. B

event a "do-nothing" Congress of the type once denounced would now be a relief, because at least it would keep the problems from being compounded. It would not be sufficient relief, however, because laws and regulations already in effect have acquired their own momentum and have an unremitting capacity for creating further mischief.

What is needed, then, is a government in which both the legislative and the executive branches are determined to look ahead by first taking an intelligent glance back. Past errors must be recognized and rectified, before larger hopes can be refueled.

The turn of the calendar may inspire some imaginations with visions of a "leave new world," but first it would behoove our leaders to consider which parts of "the good old days" can be resurrected. In short, we must repair to the past and retrieve the best of its principles.

As Patrick Henry once said, "I have but one lamp by which my feet are guided, and that is the lamp of experience." So today, we must most brightly illuminate our future by recapturing some light from the past.

COMPUTER CRIME IS ALEGED AT SOCIAL SECURITY FACILITY

● Mr. RIBICOFF. Mr. President, on March 3, 1978, in remarks in the Senate, I reported on an exercise conducted by the U.S. General Accounting Office in which GAO auditors tested the security procedures at the massive Social Security Administration computer facility in Woodlawn, Md.

Billions of dollars in social security checks are processed at the center, the largest civilian computer complex in the world.

GAO auditors found the security procedures to be lax and occasionally nonexistent. GAO warned that the installation was vulnerable to major computer fraud and terrorist attack.

Now a worker at the facility has been charged with manipulating a computer there in order to pay herself and two accomplices more than \$500,000 in disability benefits.

It is important that the Social Security Administration assure that security is adequate at this computer facility. Safeguards must be installed to prevent crime. Equally necessary are protective devices to defend this facility against terrorist attack. A major disruption in the operation of that facility's computers would cause great social difficulties.

The Washington Post reported on the alleged computer crime on February 20, 1980, in an article by Chris Schauble.

Mr. President, I request that the Post article be printed in the Record, along with my March 3, 1978, Record remarks and accompanying documents.

U.S. AIDE HELD IN \$500,000 THEFT BY COMPUTER

(By Chris Schauble)

BALTIMORE, February 19.—A worker at the Social Security Administration headquarters was charged today with manipulating the national computer at the complex in order to pay herself and two accomplices more than \$500,000 in disability benefits.

The computer, in the Baltimore suburb of Woodlawn, sends out \$1.1 billion in disability checks to 4.8 million workers and their dependents each month.

The Secret Service, which spent 18 months unsuccessfully trying to trace the money stolen through false disability claims, today

described the computer theft scheme as "very, very sophisticated."

"If there hadn't been a bank official in Philadelphia alerted to a discrepancy in an account opened there, we'd still be operating in the lull of the unknown," said Andrew E. Berger, head of the Secret Service office here.

"This was a very sophisticated scheme and the potential of the misuse [of the computer] and the lack of safeguards at Social Security is alarming. There's a potential [that] we're sitting on the tip of an iceberg with this." He said agents from Washington, Philadelphia and California are continuing the investigation.

John Trollinger, a spokesman for Social Security, said, "There are safeguards in place and we are continuously reviewing and revising our computer system."

The worker is accused of processing disability checks under numerous aliases, using real social security numbers and then erasing all records of payments from the computer before it produced a regular audit of claims and payments, Berger said.

Berger said Janet Elizabeth Bartes Blair, 29, who has worked at the agency since 1973, allegedly operated the computer theft scheme by filling out the paperwork for the computer to send disability checks to various addresses and post office boxes in Washington and Philadelphia. The two accomplices allegedly picked up the checks, cashed them through savings accounts with several banks, and, a short time later, closed out the accounts, Berger said.

None of the money allegedly obtained from the scheme has been recovered, investigators said.

Blair was arrested at her Baltimore home today after calling in sick to her office. She is still employed at the Social Security Administration, and a spokesman there said Blair was "transferred to a non-sensitive position as a result of the investigation."

She was ordered jailed in lieu of \$100,000 bond by a federal magistrate following her indictment on 43 counts of conspiracy to defraud, causing false Treasury checks to be made, and aiding and abetting forgery.

Stella Marie Abrams, 31, of Philadelphia, and Malcolm Blair, 29, Blair's brother-in-law, were charged as accomplices in the indictment returned by a federal grand jury here today. Malcolm Blair is currently serving time at Lewisburg federal penitentiary in Pennsylvania on an unrelated charge of receiving stolen Treasury checks.

Assistant U.S. Attorney David Queen said at the bail hearing for Janet Blair that she was "not acting alone" in the scheme and may have been taking orders from members of a religious sect.

Queen acknowledged that any suspicions about what happened to the half-million dollars allegedly stolen in the computer fraud scheme are just suspicions.

GAO FINDS THAT COMPUTER SECURITY IS POOR AT SOCIAL SECURITY

Mr. RIBICOFF. Mr. President, the Senate Governmental Affairs Committee has been examining computer security in Federal programs for 2 years now. As a result of the committee's investigation, the Office of Management and Budget is working to strengthen computer security procedures in Federal programs. In addition, along with Senator Percy and other Senators, I introduced legislation, S. 1766, to improve the ability of prosecutors to prosecute cases against persons accused of computer fraud.

The U.S. General Accounting Office shares my committee's concern for computer security. GAO auditors have done excellent investigations in the manner in which executive branch agencies secure their computers against theft, penetration, assault, and other forms of compromise.

The GAO has found serious shortcomings in the security procedures within the social security computer systems.

Mr. President, I ask unanimous consent that a February 21, 1978 letter from GAO Associate Director Franklin Curtis to Donald I. Wortman, Acting Commissioner of Social Security, be printed in the Record.

Mr. President, I ask unanimous consent that a March 3, 1978 letter from me to HEW Secretary Joseph Califano call Secretary Califano's attention to the Wortman letter be printed in the Record.

There being no objection, the letters were ordered to be printed in the Record, as follows:

COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C., March 3, 1978.

HON. JOSEPH CALIFANO,

Secretary, Department of Health, Education, and Welfare, Independence Avenue SW., Washington, D.C.

DEAR JOE: I wanted to call the attached report from the U.S. General Accounting Office to your personal attention.

As you know, the Senate Governmental Affairs Committee has for two years now been working to encourage the federal government, particularly civilian agencies, to improve their security procedures. I have also introduced legislation, S. 1766, which has the support of the Department of Justice, to improve the ability of the government to prosecute persons who violate computer systems.

One of the serious problems that came to light in the Committee's investigation was that the Department of Health, Education and Welfare was not adequately equipped to investigate allegations of computer crime.

The attached letter from GAO Associate Director Franklin A. Curtis to Donald I. Wortman, Acting Commissioner of Social Security, demonstrates to me the potential for computer compromise at Social Security. I urge you to increase your efforts to improve computer security throughout HEW and to take immediate steps to see that the shortcomings in security at the Social Security complex in Baltimore be eliminated. Too many of our citizens rely on Social Security for career security procedures to be allowed.

I am frankly shocked at such lax security at such a major federal installation. HEW spends more than any other federal agency. There must be a greater concern in seeing to it that the Department's computer security programs are strengthened.

Sincerely,

ART RIBICOFF.

U.S. GENERAL ACCOUNTING OFFICE,
Washington, D.C., February 21, 1978.

B-164031(4).

Mr. DONALD I. WORTMAN,
Acting Commissioner of Social Security,
Department of Health, Education, and Welfare.

DEAR MR. WORTMAN: Although the Social Security Administration has recently spent about \$500,000 to install a new security system for its computer operation, the central computer facility is still not secure. Unauthorized personnel have access to the computer room and tape vault. Magnetic tapes, disc packs, and other property can be removed without proper authorization, and blank and valid Social Security and Medicare cards can be taken from the central computer facility without question. Adequate security procedures have not been established, and Social Security has not made an in-depth study of its security needs with respect to the central computer facility.

Acquiring the new security system was a step in the right direction, and with some modifications and the development of adequate procedures, it should prove to be an

effective way of preventing unauthorized access to and exits from the central computer facility. However, there is another problem that must be addressed—preventing the fraudulent and malicious acts of persons who work inside the central computer facility. Considering the overall impact Social Security has on millions of Americans, and the results which would occur if its central computer facility's operations were interrupted, we believe that more effective control and security procedures must be established to protect both Social Security records and property, and the privacy of the American people.

Our observations were made between January 23 and February 3, 1978, as part of our "Review of Internal Controls and Performance of the Supplemental Security Income System." Our findings as well as recommendations for improving the security of your central computer facility were reported to members of your staff on February 10, 1978. A summary of our findings and recommendations are included below.

NEED TO PREVENT UNAUTHORIZED ACCESS TO AND EXIT FROM THE CENTRAL COMPUTER FACILITY

Unauthorized personnel can easily enter and exit the central computer facility in several ways. First of all, the central computer facility's turnstiles allow movement in both directions once they have been activated by a security badge. Thus several people can enter and exit from a single admission authorization. Since the security guards are not always positioned in direct view of the turnstiles, these unauthorized entrances and exits can go undetected. We demonstrated this by admitting two GAO auditors from a single authorization without the awareness of security guards.

A second way to gain access involves the use of temporary badges. Several of these valid badges can be obtained by an authorized individual and distributed to nonauthorized personnel. Personal identifiers such as social security number, name, and organization are obtained when the badge is issued; however, these identifiers are not used by the automated security system to make sure that only one temporary badge is valid for an authorized person at any point in time. During our observations, we admitted a nonauthorized GAO auditor into the central computer facility. Even with permanent authorization badges with employee pictures, security guards seldom match the person with the picture on the badge. Thus nonauthorized admittance to the central computer could be made if an authorized employee permits it.

Once inside the central computer facility, unauthorized exits can be made through the emergency exits without alarming security guards. These emergency exits are wired with electromagnetic connectors which when separated, set off an alarm. By removing the two screws at the bottom of the connectors, the doors can easily be opened without interrupting the circuit. Unauthorized personnel can thus exit and enter the central computer facility once these doors are opened. During our observations, a GAO auditor took Social Security property through one of the opened emergency doors without the security guards' awareness.

RECOMMENDATIONS

To avoid unauthorized access to and exits from the central computer facility, we recommend that:

Security guards be positioned in full view of the turnstiles, and that they be required to verify the pictures on the authorization badge with the person using it.

The security system be modified to allow only one temporary authorization badge to be valid for a person at any given time.

Emergency exit wiring and connectors be secured to prohibit tampering and thus pre-

vent unauthorized entrances and exits by personnel and property.

MORE CONTROL IS NEEDED OVER MAGNETIC TAPES AND DISK PACKS

Magnetic tapes and disk packs can be removed from the central computer facility without proper authorization because effective control procedures have not been established. Currently, before a magnetic tape can be removed from the central computer facility, a tape dispatch pass is supposed to be obtained from Tape Library Control Section personnel and presented to security guards upon exiting. We were able to remove tapes without tape dispatch passes because security guards did not check notebooks, lunch containers, and brief cases for Social Security property. Furthermore, Tape Library Control Section personnel do not control tape dispatch passes in their possession. We were able to remove 10 tape dispatch passes, and take tapes out of the central computer facility using these passes. Finally, neither Tape Library Control Section personnel nor security guards verify the actual number of tapes which are to be removed from the central computer facility with those actually taken out. From an authorization for a single reel of tape, we were able to remove an entire cart of 38 tapes—two segments of the Supplemental Security Income master file—from the central computer facility. Additionally, with respect to magnetic disk packs only certain individuals have authorization to remove them from the central computer facility. However, we were able to remove a magnetic disk pack without security guard action even though we had not been authorized to do so.

RECOMMENDATIONS

To improve controls over magnetic tapes and disk packs, we recommend that:

The use of the tape dispatch pass be discontinued, and in its place a transmittal sheet be established to show authorization for removal of tapes and disks and that both the Tape Library Control Section and security guards be required to reconcile the number of tapes by serial number.

Security guards should be reminded of the need to search notebooks, lunch containers, and briefcases of people entering and leaving the central computer facility.

MORE CONTROL IS NEEDED OVER SOCIAL SECURITY AND MEDICARE CARDS

Blank and valid Social Security and Medicare cards are not controlled within the central computer facility and therefore, can be fraudulently removed. During our observations, we found that blank Social Security and Medicare cards were readily accessible at various locations within the central computer facility. We also found thousands of both types of these cards—with valid names and account numbers—which had been discarded because a few had been misprinted. We were able to remove both blank and valid cards from the central computer facility through both the security gates and emergency exits.

RECOMMENDATIONS

In order to provide more control over these identification cards, we recommend that: Supplies of blank Social Security and Medicare cards be secured within the central computer facility.

Effective procedures be established to ensure that nonissuable printed cards be properly destroyed.

All identification cards be controlled and accounted for as they are used.

NEED FOR A COMPREHENSIVE APPROACH TO SECURING THE CENTRAL COMPUTER FACILITY

Social Security has not developed a comprehensive approach to securing the central computer facility, and no formal in-depth study detailing securing requirements and ways to meet them has ever been made. In July 1976, at the request of Social Security,

the MITRE Corporation made "A Preliminary Evaluation of the Physical Security Requirements of the Social Security Administration Data Processing Center." MITRE pointed out that most of Social Security's physical security measures have been implemented on a piece-meal basis. We agree with this finding and believe that the new automated security system is the latest example of this practice. No in-depth risk analysis has been performed to determine what security procedures should be established, and furthermore, no overall structured approach has been developed for securing the central computer facility.

Social Security's main approach has been to protect itself from unauthorized personnel having access to the central computer facility. However, it has not addressed another potential problem—preventing fraudulent and malicious acts of persons who work inside the computer room. All of the unauthorized acts which we performed during our observations could have just as easily been performed by persons who normally work in the computer room. Most persons having access to the computer room are not given a background investigation, and some of them are not even employed by Social Security.

RECOMMENDATIONS

To improve Social Security's overall security procedures, we recommend that:

A complete, formal risk-analysis be performed to determine what security procedures need to be established for the central computer facility.

After the risk-analysis, a detailed structured approach be established for security of the central computer facility.

At a minimum, background investigations be performed on all employees who work within the central computer facility, including personnel not employed by Social Security.

Please advise us of the actions you propose to take concerning our recommendations.

Sincerely yours,

FRANKLIN A. CURTIS,
Associate Director

S. 219—CHARITABLE DEDUCTION BILL

Mr. DURENBERGER, Mr. President, I urge my colleagues to join me in my enthusiastic support of S. 219, the charitable deduction bill. It was my great privilege last year to cosponsor this much-needed measure to preserve the vitality of our Nation's charitable and volunteer community.

During the past decade, private philanthropy, like all other sectors of our society, has suffered from the mounting strains of inflation. Many individuals who would like to contribute to the arts, to their church, or favorite charity can no longer justify their contributions—not when the price of essentials for daily living is steadily and rapidly rising. After paying for food, clothing, and shelter, there is little left for charities. And, I might add, no tax incentives for the millions of taxpayers who do not itemize.

Since 1970, the percentage of taxpayers using the standard deduction has grown from 52 percent to more than 75 percent today. Between 1972 and 1978, the voluntary sector had lost an estimated \$3 billion.

The major Government incentive to private giving, the charitable deduction, needs to be revised if we are to continue to have a vigorous, broad-based volun-

