S. HRG. 102-679

PRIVACY OF SOCIAL SECURITY RECORDS

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY AND FAMILY POLICY

OF THE

COMMITTEE ON FINANCE UNITED STATES SENATE

ONE HUNDRED SECOND CONGRESS

SECOND SESSION

FEBRUARY 28, 1992

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

56-983—CC WASHINGTON : 1992

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-038873-2

COMMITTEE ON FINANCE

LLOYD BENTSEN, Texas, *Chairman*

DANIEL PATRICK MOYNIHAN, New York	BOB PACKWOOD, Oregon
MAX BAUCUS, Montana	BOB DOLE, Kansas
DAVID L. BOREN, Oklahoma	WILLIAM V. ROTH, JR., Delaware
BILL BRADLEY, New Jersey	JOHN C. DANFORTH, Missouri
GEORGE J. MITCHELL, Maine	JOHN H. CHAFEE, Rhode Island
DAVID PRYOR, Arkansas	DAVE DURENBERGER, Minnesota
DONALD W. RIEGLE, JR., Michigan	STEVE SYMMS, Idaho
JOHN D. ROCKEFELLER IV, West Virginia	CHARLES E. GRASSLEY, Iowa
TOM DASCHLE, South Dakota	ORRIN G. HATCH, Utah
JOHN BREAUX, Louisiana	

VANDA B. MCMURTRY, *Staff Director and Chief Counsel*
EDMUND J. MIHALSKI, *Minority Chief of Staff*

SUBCOMMITTEE ON SOCIAL SECURITY AND FAMILY POLICY

DANIEL PATRICK MOYNIHAN, New York, *Chairman*

JOHN BREAUX, Louisiana	BOB DOLE, Kansas
	DAVE DURENBERGER, Minnesota

CONTENTS

OPENING STATEMENT

Page

Moynihan, Hon. Daniel Patrick, a U.S. Senator from New York, chairman of the subcommittee 1

COMMITTEE PRESS RELEASE

Hearing Planned on Privacy of Social Security Records, Moynihan Cites Alleged Intrusions 1

ADMINISTRATION WITNESSES

Morey, Larry D., Deputy Inspector General for Investigations, Department of Health and Human Services, Washington, DC 3

Enoff, Louis D., Principal Deputy Commissioner of Social Security, Social Security Administration, Department of Health and Human Services, Baltimore, MD 5

PUBLIC WITNESSES

Halperin, Morton H., director of the Washington, DC office, American Civil Liberties Union, Washington, DC 17

Hendricks, Evan D., editor and publisher, Privacy Times, and chairman, United States Privacy Council, Washington, DC 20

Rotenberg, Marc, director of the Washington, DC office, Computer Professionals for Social Responsibility, Washington, DC 26

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Enoff, Louis D.:
Testimony 5
Prepared statement 35

Halperin, Morton H.:
Testimony 17
Prepared statement 39

Hendricks, Evan D.:
Testimony 20
Prepared statement 49

Morey, Larry D.:
Testimony 3
Prepared statement 60

Moynihan, Hon. Daniel Patrick:
Opening statement 1
Prepared statement 72

Rotenberg, Marc:
Testimony 26
Prepared statement with attachment 74

PRIVACY OF SOCIAL SECURITY RECORDS

FRIDAY, FEBRUARY 28, 1992

U.S SENATE,
SUBCOMMITTEE ON SOCIAL SECURITY
AND FAMILY POLICY,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:06 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Daniel Patrick Moynihan, (chairman of the subcommittee) presiding.

[The press release announcing the hearing follows:]

[Press Release No. H–9, Feb. 25, 1992]

HEARING PLANNED ON PRIVACY OF SOCIAL SECURITY RECORDS, MOYNIHAN CITES ALLEGED INTRUSIONS

WASHINGTON, DC—Senator Daniel Patrick Moynihan, Chairman of the Senate Finance Subcommittee on Social Security and Family Policy, announced Tuesday the Subcommittee will hold a hearing on alleged illegal intrusions into personal Social Security records.

The hearing will be at *10 a.m. on Friday, February 28, 1992* in Room SD–215 of the Dirksen Senate Office Building.

"We are troubled by reports that a firm has allegedly bribed Social Security Administration employees to obtain private Social Security records of individuals for the purpose of selling the personal information to interested buyers. We will hear testimony on the investigation into this matter, and on what can be done to prevent this kind of intrusion into people's privacy in the future," Moynihan (D., New York) said.

The Subcommittee also will hear testimony from privacy experts on whether statutory controls are needed on the use of the Social Security number in the private sector.

OPENING STATEMENT OF HON. DANIEL PATRICK MOYNIHAN, A U.S. SENATOR FROM NEW YORK, CHAIRMAN OF THE SUBCOMMITTEE

Senator MOYNIHAN. A very good morning to our witnesses and our guests. This hearing of the Subcommittee on Social Security this morning is for the purpose of taking testimony on an investigation of alleged widespread theft and sale of personal and private records maintained by the Social Security Administration.

For the first time in now more than 55 years of the Social Security Act, we discover widespread and quite shameless invasion of our Federal record system for the purpose of obtaining information that is absolutely private; it is held in trust as the trust funds themselves are done.

This practice is not confined to Social Security records, but it seems to be most intensive in that regard. The IRS has had the

same problem where the disclosure of Federal information is a crime; it is a felony.

We are going to hear more about the nature of the subject from our witnesses, and the nature of the penalties. We have some very distinguished witnesses here. Issues of privacy arise, issues of the integrity of our Federal system arise.

We have, apparently, a new enterprise in the country called "information broker," and it appears that some of these brokers have bribed Social Security employees to reveal information; have invaded our computer systems; and, generally speaking, have violated all of the assumptions that the system has been based on, and securely based on for half a century.

One company in Tampa, FL was so bold as to mail out promotional brochures that guaranteed instant access to confidential Federal files for purposes of credit validation and other sorts of private actions.

This brochure came into the hands of investigators in the office of the Inspector General of the Department of HHS in Atlanta, and these investigators, together with the FBI, began the largest crack down on this sort of invasion of privacy of Federal records in our history.

Throughout the history of Social Security we have undertaken, as a matter of trust and law, to maintain the absolute privacy of the individual accounts.

There are 200 million Americans that have these accounts. Very shortly it will approach the whole of the population, because it is the practice now to give infants Social Security numbers at birth. I see Mr. Enoff nodding.

The Social Security number is your dog tag number in the military; it is your student ID number. I do not think it has gotten to the point where if you play football they put your number on your sweatshirt, but that day may come, too.

The amount of information and the importance of it is profound, and we have never had a hearing like this because we have never had an issue like this.

So, let us go straight to it. We are going to hear from Larry Morey, who is the Deputy Inspector General for Investigations of the Department of Health and Human Services, and Louis D. Enoff, who is the Principal Deputy Commissioner of the Social Security Administration, the Department of Health and Human Services. Mr. Enoff, would you come forward, too, sir? Yes.

Mr. Lou Enoff is well-known to this subcommittee.

Mr. Morey, I believe this is your first appearance before our committee, is it not?

Mr. MOREY. Yes, it is, Mr. Chairman. It is a pleasure to be here.

Senator MOYNIHAN. It is an honor to have you. I cannot describe it as a pleasure, because you come on very disturbing business. Which is to make the point, in half a century, we have never had a person in your position before us.

We welcome you, sir. We will take your testimony. Perhaps you would like to put your prepared testimony in the record and proceed exactly as you wish and as long as you desire. We want to hear this.

[The prepared statement of Senator Moynihan appears in the appendix.]

STATEMENT OF LARRY D. MOREY, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, DEPARTMENT OF HEALTH AND HUMAN SERVICES, WASHINGTON, DC

Mr. MOREY. Mr. Moynihan, I will be brief with my oral remarks, and I will be happy to answer all of your questions afterwards. I appreciate the opportunity to be here this morning and to testify. As you have indicated, I have submitted my written testimony for the record.

I would like to focus my opening remarks on the area of safeguarding all confidential information on American citizens contained in the Social Security Administration's computerized record systems, as well as the Social Security number fraud that we have seen rise in our country over the last few years.

Without question, Social Security has been successful in raising the quality of life for individuals over the age of 65 by providing them with a measure of income security.

In addition, Social Security provides economic protection to millions of disabled persons and their families, as well as to families of deceased workers.

Ten years ago, SSA initiated a major project to modernize its data systems in an effort to provide better services to Americans. SSA has invested over $600 million in this effort since 1983.

SSA employees can now process benefit claims and retrieve benefit and earnings information on nearly 140 million workers in minutes, rather than days.

As part of this system's modernization, SSA converted many of its files to on-line databases, which increased information accessibility to SSA employees. This has increased the vulnerability of the system and the misuse of that information.

In our Social Security investigations, we generally focus on three areas: fraud by employees, benefits fraud, and Social Security number fraud.

Based on an initial referral from the Social Security Administration, we have been investigating an increasing number of information brokers who attempt to obtain, buy, and sell Social Security data to private companies for their use in locating people, or making decisions to hire and fire people, and to lend money.

First, the broker will have one or more Social Security employees under contract. These employees sell earning histories to the brokers for about $25 apiece.

Senator MOYNIHAN. Now, just to be clear, this has to be a crime. Mr. Enoff, you join in. No employee can have a contract with a private information broker to give out this information.

Mr. MOREY. Well, it is not a signed contract, but it is an agreement with an information broker to illegally——

Senator MOYNIHAN. But it is illegal.

Mr. MOREY. Yes.

Senator MOYNIHAN. Sure. Absolutely. We are talking about—well, you will tell me whether this is a misdemeanor or a felony, but this is certainly not a contractual relationship.

Mr. MOREY. No. That is absolutely true. In fact, Mr. Chairman, thanks to you, back in 1981, you moved the misuse and altering of a Social Security number and the altering, and purloining, and counterfeiting of that from a misdemeanor to a felony.

Senator MOYNIHAN. Yes.

Mr. MOREY. And it is because of that legislation that our convictions have gone up from about 300 to about 560 per year, just in the altering and forging of Social Security cards. That legislation has been a great help to us in this fight.

Certainly, for the record, let me tell you that it is not a written agreement, but it is an under-handed scheme to defraud where these individuals will agree to produce this information.

As I said, that information will go from about $25 apiece; the price varies. When it goes back to the information broker, he then sells the information for at least $300 or more.

The brokers tend to have a set fee schedule, depending on what type of information is requested and how quickly it is needed. However, if time is not a factor, a second scheme may be used.

For a smaller fee, the broker can go through an individual who does have a contract with SSA to obtain earnings record information. These are legitimate contractors who have access to the information, and they may be an insurance company or attorneys, or other organizations.

A third scheme used by private investigators is called pretexting. The investigator calls an SSA office, usually a tele-service center, claiming to be an SSA employee from another office where the computers are down.

The tele-center service employee is requested to obtain information and read it over the telephone. The private investigator then simply writes down the information and relates it to his client.

Let me provide you with an example of a recent OIG case—the largest case we have ever investigated—involving the theft of Federal computer data by information brokers. This is the genesis of this area, and probably of the hearing; 23 individuals, including private investigators, Social Security employees, and law enforcement officers were recently indicted by Federal grand juries in Florida and New Jersey for buying and selling confidential information held in government computers.

The information released included SSA earnings information, Social Security numbers, full names, dates of birth, names of parents, names of all current and past employers, salary information, and other non-public information to unauthorized individuals.

The investigation revealed that the government employees were allegedly bribed or duped for the access to this information; some of which was then sold.

The OIG investigations set up dummy transactions through a company named Nationwide Electronic Tracking. If you read that in the paper, that is what they call NET.

We worked with them and planted names of individuals to be checked, and then alerted the SSA officials to be on guard to see how this information was accessed through the computers. As you know, indictments have been returned, and that investigation is continuing.

In addition to that activity, we also have conducted a number of reviews concerning SSA internal controls and security measures in automated data processing.

We have shared with SSA the reports which resulted from our Social Security fraud investigations. Our reports addressed various problems such as: misuse of the number; and issuance of duplicate numbers; and activities involving money laundering.

At this time I would say that we are pleased to be working with SSA to correct these problems. That concludes my oral testimony, and I am available to answer for any questions.

Senator MOYNIHAN. Well, we certainly will get to that. Let us first hear from Mr. Enoff, whom we could not ask more in the way of concern than we have had from the Social Security Administration itself about this.

I suppose it was inevitable that the day would come when efforts of this kind would take place, but they have not been shrugged off in the least by Mr. Enoff, or his associates. Let us hear from you about this matter.

[The prepared statement of Mr. Morey appears in the appendix.]

STATEMENT OF LOUIS D. ENOFF, PRINCIPAL DEPUTY COMMISSIONER OF SOCIAL SECURITY, SOCIAL SECURITY ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES, BALTIMORE, MD

Mr. ENOFF. Well, thank you, Mr. Chairman. I welcome the opportunity to be here today. And, as you have indicated, we are very concerned about the recent indictment of several SSA field employees for selling employment and earnings information.

It is a delicate balance that we are trying to achieve: to make information accessible to those who are entitled to it—generally speaking, those whom the information is about—and, on the other hand, to protect the confidentiality of that information.

With your permission, Mr. Chairman, I will summarize my remarks and submit my full statement for the record.

Senator MOYNIHAN. Well, Commissioner, exactly so.

Mr. ENOFF. Thank you.

Senator MOYNIHAN. I should have said you are a familiar person before this committee, and a very welcome one. We wanted to welcome you. We will put your statement in the record and you proceed exactly as you wish, and as long as you desire.

[The prepared statement of Mr. Enoff appears in the appendix.]

Mr. ENOFF. Thank you, sir. I want to start by saying there is simply no excuse for misbehavior by our employees in this regard. There is no place for it in Social Security. We do believe that the vast majority of our employees are honest, forthright employees.

But, with any large computer system, we have a need for security safeguards to deter that small number of persons who could be tempted to misuse their position of trust. And we do occupy positions of trust when we keep this personal data about our citizens.

While I regret that this recent incident occurred, it is important to recognize—and I think Mr. Morey made that point—that it was our state-of-the-art safeguards in the computer system that identified the misuse of the agency system and began the investigation that ensued.

Senator MOYNIHAN. Of course, it is not just one event at this point. We have a general problem of people probing our records systems. The IRS has it and you have it.

Mr. ENOFF. Yes.

Senator MOYNIHAN. You are not alone.

Mr. ENOFF. You are absolutely right. I am saying that this indictment—which is the first instance, as you pointed out, of SSA employees selling information—resulted from our safeguards.

Senator MOYNIHAN. Yes.

Mr. ENOFF. And, while it is not comforting to have the event occur, it does show that these safeguards are working to that extent.

Now, we take very seriously the responsibility to protect the privacy of the personal information in our files. And, until relatively recently, our commitment to confidentiality was relatively easy to carry out because it was so difficult to retrieve information that was stored in folders housed in record centers.

But this storage system, as you point out, also meant that local offices, or beneficiaries, or citizens who wanted information about their own account had to wait days or weeks to get the information needed to process claims or to answer a question.

Senator MOYNIHAN. Yes.

Mr. ENOFF. In the past decade, our increased computerization has made it possible for our employees to get needed information within seconds and for us to be able to send earnings and benefit estimates to citizens quickly.

So, the computerization has dramatically improved our ability to serve the public. However, it does make ensuring confidentiality more difficult.

In Social Security there are two types of computer requests, or what we call queries, that are most susceptible to misuse. The Inspector General's Office has identified this, also.

The first type of query is what we call the Alpha Index query, which gives the Social Security number that is assigned to an individual name. This Social Security number then, in turn, provides access to all information in our files about that individual.

The second type of query is called the Detailed Earnings query, which provides employer names and addresses, along with the amount of earnings each year.

Now, some outside entities are very interested in the information that is available through these two queries because that information can be used to verify credit applications or to locate individuals by obtaining the names and addresses of their employers.

We took this into account during the planning for the automation of our data files. We visited major banks and insurance companies to see how they protected their automated systems, and we built the best of these safeguards into our new systems when they were implemented in the mid- and late 1980's.

And, Mr. Chairman, I would tell you that last week, in our meetings with the National Academy of Science panel that has been reviewing our systems efforts, I asked them again if they would take a look at the security safeguards in our system.

That distinguished panel reported to me that, indeed, we have the latest, state-of-the-art computer safeguards installed for security purposes.

Senator MOYNIHAN. Well, good for you. You went to the——

Mr. ENOFF. The National Academy.

Senator MOYNIHAN. Is that the Commission on National Statistics, or one they set up for your purposes?

Mr. ENOFF. No. It is a special group that is reviewing our systems effort.

Senator MOYNIHAN. Oh. Yes.

Mr. ENOFF. Dr. Willis Ware chairs that panel.

Senator MOYNIHAN. Oh, sure. Yes.

Mr. ENOFF. If you would like, I will supply the list of the panel to you, because we had an interesting discussion about how we might, as we continue to automate, consider various safeguards.

Senator MOYNIHAN. That is good public administration to go to the National Academy and ask Dr. Ware's eminence and say, are we doing this right, and you are going to get the best and cheapest advice available.

Mr. ENOFF. We do appreciate that. Commissioner King has had them looking at our systems program generally, so we simply added this to their charter.

Now, let me just spend a minute talking about what we do to prevent access by unauthorized people. We first assign a personal identification number, or what we call a PIN, to employees, on a need-to-know basis.

That is, each person who has a need to enter the system of records has his or her own unique personal identification number. In addition, even employees who enter that system do not have access to all the files because they may need access only to some portion of the file.

So, the system prevents them from entering into those files that they do not need. We use a commercial software package that is called Top Secret. It controls access to each file and allows employees to access only the information that they need to do their particular type of job.

For instance, although I have a personal computer that I use, I cannot personally access data about wage records, because I have no need to do that in my job.

If someone contacts me with a question about his or her wage record, I call an employee who has a need to access those records on a regular basis, and, through the personal identifier, the employee is able to get that information.

Senator MOYNIHAN. Yes.

Mr. ENOFF. But there is no need for me, or someone in the personnel office, or someone in the budget office to have that information.

This widely-used package—this Top Secret software package—was evaluated by the National Security Agency in the 1980's and was found to be appropriate for SSA systems security purposes.

Senator MOYNIHAN. Oh. You brought the NSA in on your——

Mr. ENOFF. Yes, sir. That was early on.

Senator MOYNIHAN. Could I just say, that is good government. I mean, to have a job you have to do dealing with the records of 200

million Americans, and putting it on a computer, taking it out of the folders and those original—I suppose my Social Security records go back to the point where they were penned in with a pen and ink.

So, when you are doing it, go to the National Academy of Sciences and say, how does this look to you, and go to the National Security Agency and say, does this seem secure to you. And that is using the resources of the Federal Government. Nicely done.

Mr. ENOFF. Thank you, sir. The second safeguard that we have, Mr. Chairman, is the capability to monitor access to sensitive files. That is, each time that one of these sensitive files is accessed, there is an audit trail created in the system as a by-product of that transaction.

It was this audit capacity that identified this particular case initially and allowed us to refer it to the Inspector General. And this audit trail is used by our systems security officers, who are the third safeguard in our system.

Our systems security officers develop and enforce our overall systems security policy and guidelines; they monitor adherence to security plans and initiatives; and they make sure that the automated security safeguards are, in fact, working properly.

The fourth safeguard that we have is local field office management reviews of actions processed in their offices, such as requests for Social Security cards. This is to ensure that they are legitimate.

The local security officers and other management officials are taught to watch for any incident or pattern of behavior which is out of the ordinary and which may indicate that an employee is involved in some activity that might involve sale or misuse of information.

We ask our managers to see if an employee is requesting an inordinate number of Social Security cards, just to check to determine if there is some valid reason for that.

And then they notify the regional systems security officer and the Office of Inspector General if they find something that is an indication of misuse.

Our final safeguard is careful training of employees about the confidential nature of the personal information in SSA's files and the penalties for misuse of that information.

Each person who is issued a PIN certifies in writing that he or she understands and will comply with our disclosure policy. And we periodically issue reminders of that responsibility and that trust.

As a matter of fact, we have a reminder that will go out this week from the Commissioner to all employees reminding them about privacy rules, and we do this periodically.

Senator MOYNIHAN. That, again, is very nice. The Social Security Administration is not on trial here.

Mr. ENOFF. I understand that.

Senator MOYNIHAN. We are very impressed with what you do. And the volume—Mr. Morey, your testimony records this. Last year, the SSA issued 19,700,000 Social Security cards. What would that be, Commissioner; about half would be replacement?

Mr. ENOFF. It is about half. Yes, sir.

Senator MOYNIHAN. Yes. And I have been for 16 years on this committee trying to get a card that really cannot be counterfeited. And something there is that does not want that to happen, but if I have another 16 years—which I doubt—it may yet transpire.

But that card is worth money in Cuernavaca. Illegal immigrants will pay a lot for it. I mean, those cards go for hundreds of dollars.

And to people avoiding their responsibilities, the Social Security cards are counterfeited, and something in our administrations, one after the other, says they just do not want to put out a permanent piece—I have somewhere in my dresser drawers that little cardboard piece of paper I was given, good God, 50 years ago, or near thereto.

And it is still a cardboard piece of paper. You have got some fine filaments in it now. We got a statute passed. But what they did, Mr. Morey—it was not Commissioner Enoff—but we ordered them to produce a counterfeit-proof card.

They produced the same old card, which, under a microscope, the FBI can tell whether it is a counterfeit or not. But, for the purposes of an employer or anyone else, it looks the same as anything else. And the counterfeits work as well as they ever did.

How many counterfeit cards would you think are around?

Mr. ENOFF. I think the Inspector General might know better how many, but there certainly has been counterfeiting of the new card, as you indicate. But not as much as of the old card, we think.

Mr. MOREY. We have numerous cases where, after an arrest or a search warrant, we have found stacks of counterfeited cards. It is well into the hundreds of thousands.

Senator MOYNIHAN. You mean, you have people who just sell them wholesale?

Mr. MOREY. Yes, that is correct.

Senator MOYNIHAN. Or buy them in wholesale and sell them in retail.

Mr. MOREY. Technology increases for them almost as fast as it does for us, so it is difficult to keep ahead of someone who wants to either counterfeit the SSN card or alter it.

Senator MOYNIHAN. I do not want to get us off our main issue here, but there is one thing that the counterfeiter cannot overcome, which is that he is using a number which will ring a bell in Commissioner Enoff's system.

Mr. ENOFF. That is correct.

Senator MOYNIHAN. And if we had a piece of plastic which you could just run that number through and it rang up, and it would automatically and very quickly tell you that that number is not legitimate, would it not?

Mr. ENOFF. The problem that we have there, Mr. Chairman—and we have worked with the Inspector General to try and encourage State entities to tighten security in the issuance of birth certificates—is these clever bandits are selling whole identity packages; the Social Security card is one little piece.

And they start by getting a birth certificate of some individual, usually someone who has died at an early age. Most anyone can request a birth certificate for another person from a State Vital Statistics Bureau.

Senator MOYNIHAN. You write into Tallahassee and——

Mr. ENOFF. For $5 they can get a birth certificate. Then they create a whole identity package for that individual, and they match that to the characteristics

of the individual to whom they are selling it: sex, age, race, maybe.

Senator MOYNIHAN. This is getting to be an industry out there.

Mr. ENOFF. Unfortunately, yes.

Senator MOYNIHAN. I interrupted you.

Mr. ENOFF. I am sorry.

Senator MOYNIHAN. No. I interrupted you. I am sorry.

Mr. ENOFF. All right. Let me just finish by saying that we continually explore ways to improve our computer system safeguards without decreasing our level of public service.

In addition to possible changes in computer safeguards, we are considering other possibilities, including seeking legislation to increase the monetary penalties for misuse; issuing special bulletins to employees as I mentioned; and making SSA employees aware of the convictions and penalties imposed on those found guilty of misusing information.

Should these persons that are currently under indictment be found guilty, we think that we need to ensure that all employees are aware of the penalties that have been imposed. We are ashamed of it in one sense, but it needs to be known.

In conclusion, Mr. Chairman, let me say that Social Security has always made confidentiality of personal information in our file——

Senator MOYNIHAN. It goes back to 1936. You made that decision in 1936.

Mr. ENOFF. It has been a cornerstone of our policy. The agency mission is to serve the public as quickly and effectively as possible, and this requires that thousands of employees have access to the personal information in our files.

Therefore, we must continually review our safeguards and work with the Inspector General, other law enforcement agencies, and those organizations responsible for and interested in the area of privacy and safeguarding data.

I believe that the information and ideas brought out by this hearing are very helpful, Mr. Chairman. We applaud this effort to bring these issues before the Senate and before the public, and we stand ready, as always, to work with you and the other interested parties to ensure the protection and the privacy of data regarding our citizens.

I thank you Mr. Chairman, again, for allowing me to be here, and I am ready to respond to any questions you may have.

Senator MOYNIHAN. Thank you. Commissioner, let me ask you a matter that is very much in the news right now, which is the question of welfare, and the Family Support Act of 1988 which requires that child support payments be paid. And, of course, what we call welfare is Title IV of the Social Security Act.

Do you have a problem providing earnings records to other government agencies responsible for child support enforcement?

Mr. ENOFF. No, sir. We do provide information where it has been statutorily determined that that information would be helpful.

Senator MOYNIHAN. Yes.

Mr. ENOFF. And the Congress has given us authority—as a matter of fact, responsibility—to provide that information to our sister agency which administers AFDC. So, we do provide that information.

And, as a matter of fact, you would probably be interested in this. Just this morning, I saw a report on another matching operation that the Congress authorized us to begin last year with regard to those persons who have at one point in time received money from the Social Security Administration erroneously, had been overpaid, are no longer receiving Social Security, and have refused to repay the money. It is called tax refund offset.

Senator MOYNIHAN. Yes.

Mr. ENOFF. We can match computer files with the IRS in terms of numbers.

Senator MOYNIHAN. Yes. This committee did that.

Mr. ENOFF. This is the first year of operation and in the first 4 weeks of operation, Mr. Chairman, we have recouped $11 million in overpayments as a result of that simple match. So, it does work, but we are very careful that it is only used for those purposes that are defined.

Senator MOYNIHAN. Would you know offhand how many queries you have gotten from the HHS family support side with respect to child support?

Mr. ENOFF. I could supply that for the record, Mr. Chairman.

[The information requested follows:]

The Federal Parent Locator Service (FPLS is located within the Office of Child Support Enforcement (OCSE) and conducts weekly matches against the Social Security Administration's (SSA) databases to obtain employer or absent parent address information, and Social Security numbers for absent parents. During fiscal year 1991, 2,031,970 cases with Social Security numbers were submitted to SSA electronically to obtain employer and/or benefit information, and 100,197 cases without Social Security numbers were submitted to identify the correct numbers.

Section 453 of the Social Security Act provides that the Secretary of Health and Human Services shall, through the FPLS, obtain and transmit to any authorized person information as to the whereabouts of any absent parent when such information is to be used to locate such person for the purpose of enforcing support obligations against such parent. Requests under section 453 are limited to requests for Social Security numbers and the most recent address and place of employment of any absent parent. OCSE, through the FPLS, can obtain earnings information from the Internal Revenue Service and by accessing State Employment Security Agency databases.

Senator MOYNIHAN. Would you do that? We would like to know that. Because the pool, if that is the word, is probably up there at 20–30 million persons owe child support of one form or another and they are required to pay it.

Mr. ENOFF. Yes, sir.

Senator MOYNIHAN. But we are in the infancy of that effort, even thought it is 3 years old now. Do you run across that question, Mr. Morey, the use—it gets pretty public when, in the end, prosecutors take the case to court and say, this absent parent has earnings of thus and so, and, in some States now we have a formula. The States will say it is 40 percent of the mother for one child, and 50 percent for three children. So, do you run into that question?

Mr. MOREY. Periodically. What we generally run into are cases where a mother who is supporting a child will call us in an attempt to locate the husband.

Senator MOYNIHAN. Yes.

Mr. MOREY. And then we tell her that there is a procedure for that, so it is more of an information referral—informing her of how to go about——

Senator MOYNIHAN. And the procedure, what is the procedure at this point? Because here we have a situation where a person with a legitimate reason and a public interest associated with that action will call and say, can I have the information about somebody else. Now, that is a problem you have to solve.

Mr. MOREY. Well, we tell her that she can get in touch with the State authorities, and that the State can then request that information.

Senator MOYNIHAN. The State can, on her behalf.

Mr. MOREY. Yes. And then that information would be provided to the State.

Senator MOYNIHAN. I think we need to know more about that. Commissioner, could you give us an account of how that traffic is moving?

Mr. ENOFF. Sure. I think it has increased, Mr. Chairman. This is just off the top of my head from discussions with Jo Anne Barnhardt, who is the Assistant Secretary for Children and Families.

Senator MOYNIHAN. Yes.

Mr. ENOFF. But you have put some new teeth in that enforcement provision in the last couple of years. As I recall, what happens now, is that the custodial parent goes to the State, as Mr. Morey indicated, because the State more or less guarantees to collect payment from the father, so that the State can actually prosecute the father—or the absent parent, I should say—in the case where he is not making payments.

The State makes AFDC payments to the family, and then offsets that with the payments it collects from the father under the court decree.

Senator MOYNIHAN. Right. That money is owed to the public.

Mr. ENOFF. Exactly.

Senator MOYNIHAN. It is not something optional. And yet, I mean, if you were to look around and say, apart from parking tickets, what is the obligation of citizenship that is most blatantly avoided in our country, it is child support.

Mr. ENOFF. And, unfortunately, there are some ways that people try to escape by crossing State lines, and I know that States are locating them through data matches.

Senator MOYNIHAN. And changing numbers.

Mr. ENOFF. That is correct. And going bankrupt, and other kinds of——

Senator MOYNIHAN. Well, that is a public activity. You know what is going on.

Mr. ENOFF. Yes.

Senator MOYNIHAN. It would be good to have from you, if you could do it—not in the morning——

Mr. ENOFF. Sure.

Senator MOYNIHAN. An account of how the legislation has changed the situation, if it has, indeed, done so.

[Information requested follows:]

Established in 1975 as Title IV–D of the Social Security Act, the Child Support Enforcement program is a Federal/State/local effort to provide custodial parents with child support services States have the basic responsibility for administering the program, but must adhere to Federal requirements in order to receive Federal funds. Title IV–D essentially requires States to maintain a child support agency responsible for providing a variety of enforcement services, such as location of absent parents, establishment of paternity, establishment and enforcement of support orders, and collection and monitoring of child support payments. Since the inception of the program in 1975, two major pieces of legislation aimed at strengthening and improving the child support program have been enacted.

The Child Support Enforcement Amendments of 1984 made sweeping changes to the program and reflect a clear congressional mandate for States and local jurisdictions to adopt improved procedures, management practices, and legal remedies. The legislation's key provisions require critical improvements to State and local child support enforcement programs in a number of major program areas. The 1984 amendments require States to implement improved enforcement mechanisms to collect overdue support, including mandatory income withholding procedures, imposition of liens, use of bonds, reporting of arrears to credit bureaus, and the use of State and Federal tax refund offsets. States are also required to establish expedited processes for establishing and enforcing support orders.

The 1984 amendments changed the Federal incentive formula to increasingly tie Federal financial participation to State program effectiveness and to encourage collections on behalf of non-AFDC as well as AFDC families. States are required to automatically provide continued IV–D services to families going off of AFDC, without the need for these families to apply or pay a fee. The amendments also require State agencies to pursue medical support as part of any child support order whenever possible. States must develop guidelines to be used for determining support obligations. Finally, the 1984 amendments require that the Federal Office of Child Support Enforcement conduct audits of State programs every 3 years.

The child support enforcement program underwent further revision with the passage of the landmark Family Support Act of 1988. Congress mandated that States ensure that child support services are provided effectively and expeditiously by specifying standards for processing child support enforcement cases and timeframes for distributing collections. Additionally, the Act requires judges and other officials to use State guidelines as a rebuttable presumption for determining child support awards and requires that States review the guidelines every 4 years. The Act also requires States, beginning in 1993, to review and adjust individual case awards every 3 years for AFDC cases, and at the request of either parent for other IV–D cases. Under the Act, States are mandated to meet Federal standards for the establishment of paternity and to require genetic testing in all contested paternity cases. The Act requires all States to have a Statewide automated tracking and monitoring system in effect by October 1995. With two exceptions, States must provide for immediate wage withholding in all new and modified orders in IV–D cases, whether support payments are overdue or not. Immediate wage withholding must be implemented for *all* support orders issued after January 1, 1994, regardless of whether a parent has applied for IV–D services.

These legislative changes have strengthened the procedures available to secure parental support, and child support collections continue to rise. For example, collections increased from $6 billion in 1990 to $6.8 billion in 1991, a 14 percent increase. Full implementation by 1995 of the Family Support Act of 1988 should make a further marked increase in the overall performance of the child support system.

Senator MOYNIHAN. Mr. Morey, from what you have seen, here we have merely a first-time event; a large-scale invasion of the Social Security system of confidentiality.

Is there legislation we ought to be considering? Mr. Enoff pointed out in 1981 we did make this a felony. But we do not want to overlegislate; we do not want to fail to do our duty. Do you have any thoughts on that?

Mr. MOREY. When I reviewed the statutes that were charged in the indictment—they ranged from conspiracy to defraud to furnishing false statements to the government; violations of the Computer Security Act; bribery counts; and I think there were a couple of counts under Title XXVI of the Internal Revenue Service Code.

When we take a look at all of those statutes on the books, it appears that they certainly would cover this type of a problem.

It may be more important to a Social Security employee and for us if the law specifically said that if you were to disclose any Social Security database information that you were in violation of a specific title under the law. This may bring home more of a point with the employees.

For example, I do not think any of these employees thought that disclosing SSA database information was a conspiracy. I think that they felt that they were certainly divulging information. I question whether or not they even thought about the tax implications of it, or the disclosure from the computer.

But if they knew for a fact that Title XXVI or Title XVIII was specifically for releasing information, it might be more important to them.

Senator MOYNIHAN. There is an old-time member of this committee not presently serving who is celebrated for his observations who once said, "I am against any conspiracy I am not part of."

But I think it is a fair point, that an employee of the Social Security Administration might not know what the legal encumbrances are and would do something that might seem friendly, even, is, in fact, a conspiracy and a felony under Federal statute.

Mr. Commissioner, you do pass that information around.

Mr. ENOFF. Yes, we do, Mr. Chairman. As a matter of fact, I will make available to you the statement from the Commissioner that we intend to release this week. And we can make that available. And we do say that it is punishable by a penalty of a fine up to $5,000 and imprisonment for 5 years.

Senator MOYNIHAN. Yes.

[The statement follows:]

THE COMMISSIONER OF SOCIAL SECURITY,
Baltimore, MD, February 28, 1992.

MESSAGE FROM THE COMMISSIONER TO ALL SOCIAL SECURITY ADMINISTRATION EMPLOYEES

SSA has a unique role among Federal agencies, in that millions of people depend on us for financial protection. To carry out our mission, we have been entrusted with personal information about Social Security number holders, and about persons who have applied for or are getting benefits. All of this information is confidential, and may only be disclosed:

- With the consent of the individual to whom it pertains, or
- When disclosure is specifically allowed by statute or regulation.

We must ensure the importance of protecting the confidentiality of SSA data in all of our day to day work. This includes taking and developing claims, responding to inquiries from members of the public or other government agencies, planning studies, and preparing agency policy.

PROTECTING CONFIDENTIALITY

SSA's collection and use of personal data to administer our programs is governed by the Privacy Act, which gives individuals some control over the records a Federal agency collects about them and over the use made of the records. It lists the situations in which we can disclose personal information from our records and requires us to:

- Collect only information needed to administer our programs, and
- Tell the individual why we need information, and what uses we may make of the information.

Information can be shared within SSA as necessary to perform our responsibilities. However, we must guard the confidentiality of our records when we deal with other agencies or individuals. SSA should collect and disclose only the minimum amount of information necessary to administer our programs.

CRIMINAL PENALTIES

The law provides criminal penalties for individuals who willfully and knowingly disclose information without proper authorization. These penalties include a fine of up to $5,000 and imprisonment for 5 years. Agency employees may also be subject to dismissal for violating SSA's rules regarding confidentiality.

EXAMPLES OF INAPPROPRIATE USE OR DISCLOSURE OF INFORMATION

You should not use SSA records to:

- Obtain or release information about celebrities, sports figures, friends, relatives or coworkers for non-program purposes;
- Assist friends in filing income tax returns; or
- Locate or release individuals' addresses for non-program purposes (such as planning class reunions).

Also, never disclose the contents of a beneficiary's folder to a third party without express written permission from the beneficiary or unless allowed by agency instructions. The instructions provide additional limitations on disclosure by telephone.

SYSTEMS SECURITY

The Social Security Administration's Systems Security Officer (SSASSO) is responsible for ensuring the security of SSA records in the systems environment. This includes establishing safeguards to protect against unauthorized use and disclosure of SSA information. The SSASSO is also responsible for ensuring that systems security breaches are investigated and appropriate action taken.

IF YOU NEED FURTHER INFORMATION

A summary of the statutes, regulations and SSA policy regarding privacy is in POMS, Part 02, Chapter 33. If you have a question that is not answered in POMS, contact your component's privacy coordinator. Each component has a coordinator to take questions and to refer them, when necessary, to the SSA Privacy Officer in Baltimore.

If you have any security questions concerning the use of SSA's systems, please send them to the SSASSO, 3208 Annex Building, 6401 Security Boulevard, Baltimore, Maryland 21235.

REPORTING ABUSES

You should report any observations or concerns you have to your manager, security officer, or, if you prefer, you may report anonymously through the Office of Inspector General Hotline at 1–800–368–5779.

GWENDOLYN S. KING, *Commissioner of Social Security.*

Mr. ENOFF. But I think the point Mr. Morey makes is that maybe it should be more specific—I do not know exactly which statute this comes from, but something more specific. And we certainly would not oppose that if something comes out of this committee.

Senator MOYNIHAN. Why do you not talk about it? Look, we are not here to harass any Federal employees. These are good public servants. But they have a right to know what the law is as it affects them.

Mr. ENOFF. Absolutely.

Senator MOYNIHAN. I mean, they have a need to know. All right. Look, we are going to get some of that information we asked you about.

Mr. ENOFF. Yes.

Senator MOYNIHAN. We are going to watch this closely. Something has happened. We suddenly find that people are invading the privacy of the Social Security contributors.

We are probably going to find some compu'er hackers at it, and you have already got your Top Secret system to block that. It is not a one-time event. I think we have a new situation here, and we will just keep after it. This is an oversight hearing.

Mr. Morey, we want to thank you, sir, and thank the Inspector General, for your efforts. Keep us abreast. If you think there's legislation you need, you tell us. And, Commissioner, thank you, sir, as always. Thank Commissioner King for making you available to us.

Mr. ENOFF. Thank you.

Senator MOYNIHAN. And I know that you have asked if you could stay around and hear the next panel, and you most certainly can.

Mr. ENOFF. Thank you.

Senator MOYNIHAN. If you need a cup of coffee, there is coffee in the back. Thank you very much, gentlemen.

We are going to have a second panel of concerned individuals, representing the fact that there is more of this difficulty of invasion of privacy. Just as there are more confidential records; the one follows the other.

We are going to have a panel consisting first of all of our good friend, Morton Halperin, who is the Director of the Washington office of the American Civil Liberties Union; Evan Hendricks, who is Editor and Publisher of Privacy Times, a journal indicative of the times, and a Chairman of the United States Privacy Council. And, finally, Marc Rotenberg. Is it Rotenberg, sir?

Mr. ROTENBERG. Yes.

Senator MOYNIHAN. Would you come forward? He is the Director of the Washington office of Computer Professionals for Social Responsibility, and we welcome you; all three. I believe, Mr. Hendricks and Mr. Rotenberg, this would be your first appearance before the committee.

Mr. HENDRICKS. That is right.

Senator MOYNIHAN. Well, we are very happy to have you. It is not the happiest of subjects to bring you here, but, perhaps, is one of the most important ones. The right to privacy is a constitutional right in our country.

It is not an option the government has; it is a responsibility it must perform. Before anything else, privacy is a guarantee to the right of citizenship to the American people, and no one must be more concerned that it existed than the Federal Government with its own records.

I want to make clear one thing that we cannot say too often: the 200 million Americans with Social Security records need to know that they, individually, can get them anytime. I think, Mr. Rotenberg, you people refer to accessing the file.

I mean, you can get your Social Security records; what you contributed; what your employer has contributed; what your benefits would be, just by asking—and that is a matter of right, which this committee insists on—but nobody else, excepting, again, the prosecutor seeking to enforce child support.

And so, as with any large file, there are variations. So, let us hear about this and your various concerns and thoughts. First, as it is recorded, Mr. Halperin. Good morning, sir.

STATEMENT OF MORTON H. HALPERIN, DIRECTOR OF THE WASHINGTON, DC OFFICE, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON, DC

Mr. HALPERIN. Thank you, Mr. Chairman. It is always a pleasure to appear before you. I think, in fact, this is my first appearance before the Finance Committee, although I have had an opportunity to testify before you——

Senator MOYNIHAN. Well, we keep running into you all over Capitol Hill.

Mr. HALPERIN. All over the place.

Senator MOYNIHAN. You will forgive my confusion.

Mr. HALPERIN. I had the same thought, Mr. Chairman. And it is always a pleasure. I should say that I am appearing both for the ACLU, and, in fact, on behalf of Janlori Goldman, who is the Director of the Privacy and Technology project in the Washington office, and who, unfortunately, could not be here.

So, I have the pleasure of presenting this statement on behalf of the ACLU. And I would like to ask that our full statement be made part of the record.

Senator MOYNIHAN. Of coarse. And Janlori Goldman, the Director of the Privacy and Technology Project of the ACLU. Good. Thank you.

[The prepared statement of Mr. Halperin appears in the appendix.]

Mr. HALPERIN. Mr. Chairman, we are concerned, as you are, and, as I know the Commission is, about the recent arrests of government employees for selling confidential information.

These arrests bring to light the growing problem: the increasing demand for detailed sensitive information by employers, by insurance companies, and others; coupled with what appears to be the relative ease with which insiders can disclose and exchange this information and which seems to have created something of a market in black-market confidential information.

And, obviously, we do not know the full extent of that, but once you find out that some of it exists, you become concerned.

I should say, Mr. Chairman, I recently had occasion to get my own Social Security record and I was both pleased at the ease with which I could get it, but I must say it brought home to me how much information about me is in a government file, and, therefore, the concern that we all have about that disclosure.

I want to deal briefly with three issues. One is the unauthorized disclosure of the information; but second is disclosure of information which has been held to be authorized, but which, nevertheless, raises problems; and the disclosure of information within the private sector and the interaction between that and the Social Security number.

The Privacy Act, as you know, was meant to deal with this set of problems, at least as far as government information is concerned. And I suspect that the citation of a criminal penalty in the Social Security agency memorandum was to the Privacy Act.

At least that would be one place where criminal and civil penalties for the disclosure of this information would exist. But the Privacy Act has turned out to be much less effective than I think the Congress intended and hoped when it enacted it.

It has turned out, at best, to be a set of procedural hoops that agencies have to go through before they collect and then share information with other agencies, and, indeed, with the private sector.

We think that these sales that we now know about illustrate the widespread and troubling problem of insider disclosure of this information: people who have access to personal information and have an opportunity, therefore, to give it to unauthorized people, which is compounded by the fact that much Federal agency information is shared with local police and, in some cases, with private industry as well.

We believe that this committee, and other committees of the Congress, ought to look at the issue of whether the Privacy Act should be strengthened in terms of the civil and criminal penalties, and, perhaps, making it clear that they apply broadly to any person who gets authorized access to records covered by the Privacy Act, or who gets access as a result of being a government employee—because you sometimes have situations where the person's access to the particular records is not authorized, but they are able to get that unauthorized access because they are government employees.

And we think agencies should be required to do what the Social Security Administration has apparently done on its own, which is to put in safeguarding procedures, including audit trails and logging methods of the kind that were described there, and that there ought to continue to be vigorous oversight by OMB, and Congressional committees, of the Privacy Act.

As I have said, Mr. Chairman, there is a separate but equally important issue of the authorized disclosure of government information as the Privacy Act has been interpreted.

As you know, the basic principle of the Privacy Act was supposed to be that no information would be disclosed except when specifically authorized by statute for the purpose for which the information was collected.

Unfortunately, among the exceptions that Congress wrote into that was the so-called "routine use" exception. And what has happened is the routine use exception has virtually swallowed the general rule against disclosure by being interpreted to be that if it was compatible with the purposes for which it was collected, it could be disclosed.

And this has been interpreted so broadly, we believe, to destroy the original intent of the act, and the principles of the act.

Senator MOYNIHAN. But you will be sensitive to the fact that we keep records in order to look them up.

Mr. HALPERIN. We keep records to look them up for the purpose for which they are——

Senator MOYNIHAN. How much money is coming to you.

Mr. HALPERIN. Absolutely. And that clearly is——

Senator MOYNIHAN. You can have an appendectomy that needs to be checked up on in 18 months, or whatever.

Mr. HALPERIN. Absolutely. I mean, for uses for which the information is gathered, the information should be available. The prob-

lem is that when it gets used for other related purposes without specific Congressional authorization——

Senator MOYNIHAN. Right.

Mr. HALPERIN. You have a swallowing up of the principle that it should only be used for the purpose. Because there are two sides to that.

It needs to be available effectively and accurately for the purpose for which it is collected, and that is less of a problem with Social Security records, as far as we know, than it is, for example, with arrest records, which are notoriously inaccurate as to what is actually the disposition in those records.

Senator MOYNIHAN. Yes. Yes.

Mr. HALPERIN. But the second problem is to make sure that there is not authorized disclosure, but, for purposes which were not the original ones, particularly without the Congress considering each one and deciding by legislation that it ought to be done, as you have done with the parent who has not made child support payments.

The other problem I want to focus on is the question of personal information held by the private sector. And we think that, while Congress has done some things to protect that information, that much more needs to be done.

Currently, Congress is considering strengthening both the Fair Credit Reporting Act, which we think urgently needs to be done, as well as the Electronic Communications Privacy Act. And we think those efforts are both overdue.

But we think, in addition, legislation needs to be passed to enforce privacy for medical insurance and personnel records.

Finally, Mr. Chairman, we have long been concerned about and opposed to the growing use of the Social Security number as a national identifier, and recent proposals to move beyond that to a specific national identification card.

As you know, despite the efforts of Congress to limit it, the Social Security number has become a de facto national identifier for many purposes.

Clearly, the use of that number makes it easier to retrieve information from systems, but we believe that a number of abuses have occurred because of the great use of these numbers in the private, as well as the public, sector.

As you know, Congress put a stop a few years ago to efforts to the practice of the Social Security Administration selling verification of those numbers to the private sector.

Senator MOYNIHAN. Well, we found out about that. Sure.

Mr. HALPERIN. Yes. But there still continues to be use of the Social Security number in private sector in ways that we think are inappropriate

For example, we include in our statement an advertisement by TRW Credit Data, which, in effect, holds itself out to help people search for former customers, for college alumni, or missing shareholders, and suggests that the way that that should be done is to give TRW the Social Security numbers of the people that you are looking for, and they then use their files to track these people down.

We think that that is an inappropriate use of the Social Security number, and one that Congress ought to consider putting a stop to.

We think, in fact, we should try to go back as far as we can to the notion that the Social Security card is for the purpose of recording contributions to Social Security and for certain other limited purposes that Congress may, by statute, identify—such as child support—but that Congress ought to try to begin to move us back away insofar as it can from the use of that as a universal identifier.

Mr. Chairman, we are pleased to have the opportunity to participate in this panel, and I would be happy to respond to your questions.

Senator MOYNIHAN. Yes. We will return to that TRW, but let us go through, as is our practice. Mr. Hendricks, good morning, sir. We welcome you.

STATEMENT OF EVAN D. HENDRICKS, EDITOR AND PUBLISHER, PRIVACY TIMES, AND CHAIRMAN, UNITED STATES PRIVACY COUNCIL, WASHINGTON, DC

Mr. HENDRICKS. Thank you very much, Mr. Chairman. It is a pleasure to be here. As you say, it is not a happy issue to be focusing on, but it is an important opportunity because what we are really talking about is the privacy of information of hundreds of millions of Americans.

Senator MOYNIHAN. Yes. Two hundred million.

Mr. HENDRICKS. That is quite a database.

I applaud the U.S. Attorneys and the IG's for the actions they have taken; it is the first concerted effort. But I fear that this is the tip of a very, very unseemly iceberg.

Mainly because for years this has been acknowledged commonly as the kind of thing that everyone knows is happening, but nobody has done anything about it, or nobody has proved.

In the book that I wrote, "Your Right to Privacy," which is part of the series of ACLU handbooks on citizens' rights under the law, the last chapter quotes private detectives as saying that, despite the laws, if the money is there, they are able to uncover any sort of personal information, including Swiss bank accounts; including the contents of bank deposit boxes. It is a very threatening situation.

How did it arise and what led to the situation which is the subject of this hearing? I think a couple of reasons. One is the ill-conceived expansion of the Social Security number, and two——

Senator MOYNIHAN. By expansion, you mean the use more widely in society. The Social Security number is the same number we started giving out from the beginning.

Mr. HENDRICKS. That is right. I do not mean they have added more numbers. I mean that it is being used in more contexts and it has been authorized for additional purposes. And I would like to touch on that for a minute, too.

I was glad that Morton Halperin focused on the weakness of the Privacy Act and the poor oversight of it by the Office of Management and Budget, and that has created a sort of a "cowboy" atmosphere in which some people with access to personal data feel anything goes.

The earlier witness from the IG's office said that these people did not realize that they were part of a conspiracy. They were not really conscious that they were doing anything wrong. This relates directly to the fact of poor enforcement and lack of training under the Privacy Act.

Just to add an exclamation point: this was the first major attempt to enforce individuals' expectation of privacy in their government-held data, but the authorities did not even bother to charge those indicted under the Privacy Act.

And you will note that they did not mention the Privacy Act in their testimony. This is because the only criminal sanction available under the act is a misdemeanor, and they prefer to prosecute under felony.

So, they had to go looking through the maze of other laws to find the kinds of charges which should be available under the Privacy Act. I agree wholeheartedly with Morton Halperin that we need amendments here.

What about the individuals whose information was pulled illegally? Again, because the Privacy Act is weak, individuals have a very difficult time jumping through legal hoops to collect any civil remedies.

While I understand this is not the jurisdiction of the subcommittee per se, a recommendation from the subcommittee would go a long way towards getting the other subcommittees to move on this. There is legislation pending.

Senator MOYNIHAN. A fair point. A fair point. We record that the Inspector General looked around for the most severe statutes he could find, not the least.

Mr. HENDRICKS. Yes.

Senator MOYNIHAN. I had not realized that the Privacy Act only extended as far as a misdemeanor.

Mr. HENDRICKS. Right. And we can see now it is a much more serious matter. In earlier times, the information was not so valuable; it was not as easy to get. But times have changed, and we must adjust the laws to keep pace with the advance of technology.

Senator MOYNIHAN. Yes.

Mr. HENDRICKS. Statutory protections are very important because—and most people do not realize this—under our constitution we do not have an information right to privacy.

That means in 1976 the Supreme Court ruled that when you open a bank account, for instance, even though the information is about you, it belongs to the bank, and the bank is free to give it out to whoever they wish.

If you want privacy, you either take the cash and stick it under the mattress, or you persuade Congress to act and put in place statutory protections. The Berger Court reasoning that when you give the information to the bank, you are surrendering it to the flow of Commerce.

Now, I believe that the Social Security number is really a case study in the erosion of privacy because of the expansion of its use and its authorization in the context that I have mentioned.

You will remember, Mr. Chairman, that the Social Security card said that this is not to be used for identification purposes. That

could go down as being one of the traditional lies to the American people on par with "your check is in the mail," perhaps.

Because it has been expanded for uses of tax purposes, and it has been picked up by the driver's license agencies; it is now required to be used by banks to report interest; and, as all those purposes were being advanced, we never had anyone on the other side of the coin arguing the privacy perspective.

This goes to another issue that I would like to touch on briefly: the need for an independent data protection office that can make that case, because there are always competing interests——

Senator MOYNIHAN. Before you go by that—and take all the time you want—I want to be clear that the history of that statement at the bottom of the card, "not to be used for identification," comes from the sensitivities and the concerns of the people who founded the Social Security Administration in the middle of the 1930's when Nazi Germany had an identification card; it began in Europe.

And those persons who opposed the general idea of Social Security itself said, you see, they are setting up an identification card, and there was much hoopla that went on about that. It was just plain concern for the issues that you raised that this statement was put on the card.

But it was inevitable that, in time, people would find it in their interest to use their Social Security number to explain who they are.

Mr. HENDRICKS. Yes. Absolutely. But I think——

Senator MOYNIHAN. It was not a lie, it was—in the end, what the founders of Social Security hoped would not happen did happen, but it was not their intention.

Mr. HENDRICKS. Right. And I think the example of Nazi Germany is an excellent one in terms of how personal information can be misused for the most horrendous types of harassment, and persecution, and murder.

That is why, in Germany, for instance, they have a very high level of consciousness about their Census data, and other privacy issues as well. That could be the subject of another hearing, I am sure.

But in talking about the ill-conceived uses of the Social Security number, there are two proposals that were recently shot down, and I am very happy about that because I think it symbolizes a turning of the tide and maybe the beginning of the reversal of the expansion of that number.

One was this immigration proposal that would have created a national work identity card. A job applicant would have had to present this to prove he was here legally to work. One idea was to create a call-in database for employers.

We always had a tradition of opposing a national identity card here, and the proposal was shot down.

There was a more obscure proposal this year that would have created a bank insurance fund and the Treasury Department would have taken the Social Security numbers of every American's bank account and put it into a nationwide computer to ensure that if a bank failed, no one would be paid more than the $100,000 of bank insurance to which they were entitled.

It was sort of a ludicrous proposal that was eliminated, I think, on the House side, in the Bank Insurance Fund legislation.

Senator MOYNIHAN. But I am going to take the liberty of interrupting again.

Mr. HENDRICKS. I welcome your interruptions, Mr. Chairman.

Senator MOYNIHAN. When we set out to make a tamper-proof Social Security card—one that is plastic, if that would be the optimal arrangement; one that could easily be checked; is this number a legitimate number—one of our concerns was that Hispanic Americans approaching an employer who has increasing penalties for employing illegal aliens.

Well, they look at the individual and he is Hispanic, and they look at the Social Security card, and it is a battered piece of cardboard that could be printed in anybody's basement, and they say, well, maybe we do not need to hire this person.

Mr. HENDRICKS. And then you would have outright discrimination in that context.

Senator MOYNIHAN. Yes.

Mr. HENDRICKS. Again, as Morton Halperin mentioned, the Social Security number has become an identification number of choice in the private sector in many contexts, and that is where it is not really mandated, and that is where I think, again, that we could turn it around. And I receive several dozen complaints per year from people who are just very irate about how the purposes for which Social Security number is being asked.

If I say it is a cowboy atmosphere, then the corollary to that is if you want to protect your privacy, sometimes you have to act like Jesse James, a lone gunman, to protect your privacy.

A New Jersey man named Don Pensa who just did not want to give out his SSN. When the DMV in New Jersey asked for it, he convinced them that they could use another number.

When the FAA wanted it for his pilot's license, again he debated with them and stopped them. When the fuel oil company said they would not deliver him fuel unless he gave it, he said, I will go to another company, and they changed their mind.

Unfortunately, his health insurance company, the health insurance company refused to give him health insurance unless he gave them the Social Security number. He got into a 5-month long battle with them, and, with the help of a little publicity, he was finally able to force the insurance company to back down. Another example of something I learned recently and information I would like to turn over to your subcommittee, is that a Long Island man told me that he was being forced to sign a waiver for all of his Social Security retirement benefits for an insurance company that he has a disability policy with.

Senator MOYNIHAN. Oh. We would like to know about that.

Mr. HENDRICKS. Yes. And he had been very frustrated in trying to do something about this. And now that I am here, I realize that this is where he can get the most help. So, I will provide that information to your staff. It is a very troubling example.

Senator MOYNIHAN. Yes, indeed. Just hold one second, will you?

Our distinguished counsel, Mr. Lopez, is almost certain that that is illegal, and we will find out soon. I see Mr. Enoff nodding his

head in agreement. That is illegal. I want to know the name of that company.

Mr. HENDRICKS. Yes. Well, we will gladly provide you all that information and be waiting to report on the activities.

Again, I thank Morton Halperin for mentioning this Social Security Administration match that they were doing secretly under the former Commissioner with the TRW and the Citicorp.

One thing that Privacy Times discovered by working with the Senate Aging Committee staff is that when Citicorp, for instance, submitted a database of 3 million people to match with SSA, nearly 1 million of the Social Security numbers turned out to be incorrect, presumably in Citicorp's database.

And TRW did a 150,000-person database, and, again, about one-third of the numbers turned out to be incorrect. So, that points to the issue that this is not really a reliable personal identifier.

It is not a reliable personal identifier, one, because it is used for other purposes than it is originally intended, and, two, because, as we know, SSN's are stolen, lost, shared, intentionally altered, or accidentally transposed.

Another issue is emerging in Fair Credit Reporting Act amendments, as the credit bureaus are pushing very hard to make the Social Security number an official identifier. This despite the experience that TRW had, and that we in the privacy community are very much opposed to it.

The Privacy Act has a section on the Social Security number, but the whole point of my testimony is to show that they are virtually meaningless.

In terms of general solutions, again, Morton Halperin has already said that about amending the Privacy Act and a recommendation from this committee would be useful there.

I think we can go further and start exploring the possibility of a moratorium on the use of all SSN's that are not already authorized by law. That will give us a pause and a chance to find out where we are and maybe come out with a good policy.

Borrowing an idea from something that is in the Freedom of Information Act amendments, I think that any proposal in the future to expand the use of the SSN must by dicta come before the subcommittees of jurisdiction; this subcommittee and the one in the House, so the proposal can have the benefit of your expertise, and you can weigh all the competing interests and really make the right policy decision.

It is when these policies are slipped through the back door and go through other subcommittees that really do not have your expertise that sometimes we get bad policy in this area.

Amending the Privacy Act—and just a word on the issue of a data protection board. This is a proposal that is introduced by Congressman Wise in the House.

I have studied other countries as well, and in Canada, the Privacy Commissioner then, John Grace, did a study of how their social insurance number, appropriately called the S-I-N, or SIN number, was being used throughout their Federal Government.

And he found, in a lot of cases, they did not need to use this SIN number, and he recommended to the government that it stop using

it in these contexts. And, sure enough, the government agreed, and they rolled back the use of the SIN.

And, so, I believe that this data protection board can play a very appropriate role. I think someday we will have one, and I hope that we can expect your support as we reach that point that it is near enactment.

What the subcommittee can do now, in closing—I think all we have is this anecdotal data about SSN use. What we would like to see is perhaps a two-track study by the appropriate research office of Congress—and that could be GAO, OTA, CRS—to explore the extent to which Federal, State, and local agencies are complying with the Privacy Act section which deals with the Social Security number.

And the second track would document the extent which the private sector organizations are using the SSN as an identifier when they are not required by law.

Then I think also, too, the pressure on government to do these sort of verification schemes for people outside the government will always continue, and I think a commitment from SSA that these sort of proposals will not be endorsed is important.

In closing, my colleague to the right likes to quote Louis Brandise. I like to quote Supreme Court Justice William O. Douglas, who is more from my neck of the woods out West.

In his dissent in the *California Bankers' Association* case in 1974, in which he opposed a law that required the recording of all checks and bank accounts.

He said, "It would be highly useful to governmental espionage to have like reports from all our book stores, all our hardware and retail stores, all our drug stores.

These records also might be useful in criminal investigations. A mandatory recording of all telephone conversations would be better than the recording of checks under the Bank Secrecy Act if Big Brother is to have his way.

In a sense, a person is defined by the checks he writes. By examining it, the agents get to know his doctors, his lawyers, his creditors, political allies, social connections, religious affiliation, and educational interests, the papers and magazines he reads, and so on, ad infinitum."

And this is the key. "These are all tied to one Social Security number. And now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat by pushing one button to get, in an instant, the names of 190 million Americans who are subversives or potential and likely candidates."

Mr. Chairman, I have gone way over my time. I apologize for that. But thank you for this opportunity. I would be happy to answer any questions.

Senator MOYNIHAN. Thank you. Those were very useful thoughts that we have the GAO take a general look at this whole general subject. Before another moment passes, however, I want to get that statute clear here.

This is the Social Security Act, Section 207: "The right of any person to any future payment under this title," which is to say, Social Security, "shall not be transferable or assignable, at law or in

equity, and none of the moneys paid or payable or rights existing under this title shall be subject to execution, levy, attachment, garnishment, or other legal process, or to the operation of any bankruptcy or insolvency law."

Whatever that insurance company on Long Island is doing, they had better—maybe they do not know this.

Mr. HENDRICKS. The insurance company is in Kansas; the constituent is in Long Island. But I think he is about to get served very well.

Senator MOYNIHAN. Well, they had better stop.

[The prepared statement of Mr. Hendricks appears in the appendix.]

Senator MOYNIHAN. And now, Mr. Rotenberg, we welcome you, sir, on behalf of the Computer Professionals for Social Responsibility.

STATEMENT OF MARC ROTENBERG, DIRECTOR OF THE WASHINGTON, DC OFFICE, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, WASHINGTON, DC

Mr. ROTENBERG. Thank you very much, Mr. Chairman. The computing profession has a longstanding concern about the development of adequate privacy protection for computer systems containing personal information.

Senator MOYNIHAN. I am going to put your whole statement in the record and you proceed just exactly as you wish.

[The prepared statement of Mr. Rotenberg appears in the appendix.]

Mr. ROTENBERG. All right. Thank you. The recent events about the sale of personal information held in government databases are, as my colleague to the left suggested, just the tip of the iceberg.

And, in fact, I would go a step further and say that this problem is much more far-reaching and complex than may have been previously suggested.

There is a temptation, for example, to suggest that an appropriate solution might be the expansion of criminal codes to restrict the sale of government information, or, perhaps more monitoring of government employees to see what their record-usage practices are.

But, in fact, I think what you are seeing is the result of dramatic changes in computer technology and business practices that have evolved during the past 20 years.

And the most critical change which is largely responsible for the birth of this information broker industry is the growing misuse of the Social Security number by the private sector.

Senator MOYNIHAN. Now, you are the third person on this panel to use the term "misuse" or some variant thereof. That is new.

Mr. ROTENBERG. Let me try to explain that, Mr. Chairman. In 1973, the then Secretary of HEW, Elliott Richardson, asked Willis Ware to convene a panel to assess some of the privacy implications of the rapid computerization of government recordkeeping systems.

Senator MOYNIHAN. We have heard enough to indicate that they are still working with Dr. Ware.

Mr. ROTENBERG. Yes. Dr. Ware's panel came back with a number of recommendations, many of which were incorporated into the Privacy Act of 1974. One of the critical recommendations that was

contained in the 1973 HEW report was that strong restrictions be placed on the use of the Social Security number.

In fact, Section VII of the Privacy Act reflects the findings of the HEW report in making a requirement that any agency which asks for a person's Social Security number must do three things: it must first specify the statutory authority for the request; it must, second, indicate whether the request is mandatory or voluntary; and, third, it must explain the reason or the purpose that the request is being made.

Moreover, that particular section of the Privacy Act goes on to make clear that if a person chooses not to disclose his or her Social Security number, no harm should, therefore, result.

Now, these are a very good set of principles and they were intended to constrain the use of a Social Security number to limit its misuse.

Unfortunately, what has happened in the last 20 years is two flaws in the act's structure have come to light. The first flaw is that there has not been adequate oversight.

It was clear in 1973 that it was going to be necessary to create an independent privacy oversight committee to realize the principles that were contained in the act. But, at the last moment, that particular provision was removed.

And it is for this reason that many privacy advocates today believe that a data protection board should be established.

Senator MOYNIHAN. Which committee? Is it government affairs? Margaret Malone thinks it may be. The Privacy Act came out of Government Affairs.

Mr. HALPERIN. The Government Affairs Committee has jurisdiction.

Senator MOYNIHAN. And they had thought to have a subcommittee on oversight of this particular measure.

Mr. ROTENBERG. They intended to create an independent agency.

Senator MOYNIHAN. Oh. The equivalent of the Canadian Privacy Commission.

Mr. ROTENBERG. Precisely.

Senator MOYNIHAN. I see. I see. I understand.

Mr. ROTENBERG. But that provision was removed from the bill before passage and the authority was left at OMB. And I think that is one of the sources of the problem.

The second source of the problem is the rather dramatic change in recordkeeping practices in the private sector during the last 20 years, such that the Social Security number has increasingly been used as an identifier of personal records.

Now, it is a truism, certainly, that the Social Security has become a universal de facto identifier in the United States. But that merely restates the problem, which is to say, that any person who is in possession of a Social Security number is able to acquire a great deal of information about the subject to whom the number is assigned.

And, if you look at the NET brochure, for example, which you mentioned in your opening statement, you will see that many of the services that that information broker provides are made possible once the Social Security number is provided to the company. But for the provision of the number, the services could not exist.

So, I am emphasizing at this point that this is a problem that really needs to be addressed. This is the dynamic; the underlying engine that has given rise to the tremendous demand for personal information.

Now, briefly then, I see three steps that might be taken at this point to try to curb this problem. And, as I suggested earlier, I think you are seeing what is really the beginning of many similar incidents that are likely to come about in the next few years.

Senator MOYNIHAN. Yes.

Mr. ROTENBERG. The first recommendation is the creation of the Data Protection Board. I view this initiative as absolutely critical right now.

Senator MOYNIHAN. Was that the provision that was omitted?

Mr. ROTENBERG. Yes. Representative Bob Wise has a bill in the House right now. I do not believe it has been introduced in the Senate.

But this step must be taken to begin to provide some of the expertise and resources that is necessary for the agencies to develop stronger privacy protection, and also to work with the private sector to explore alternative recordkeeping systems.

The second recommendation that I would make is that the principles contained within the Privacy Act regarding restrictions on the use of the Social Security number be extended to the private sector, and, specifically, that private sector organizations not be permitted to obtain a Social Security number absent statutory authority.

The goal is not to prohibit the flow of information that is necessary for a proper purpose; the goal here would be to try to restrict the use where there is no clear purpose that has been established or no statutory authority for the request.

Now, I should mention that many organizations—and this is true in government as well—say that they need the Social Security number because that is the way that they have designed their recordkeeping systems.

But we are finding increasingly that when you go to an organization and say, look to an alternative identification scheme, organizations are able to develop them.

And, in fact, there was an item yesterday in the Washington Post which said that the State of Maryland has decided that for their motor vehicle record system they are no longer going to use the Social Security number as the identifier——

Senator MOYNIHAN. Oh, really?

Mr. ROTENBERG. Because there has been concern about the privacy implications of the SSN. Similarly, other States are beginning to re-think their recordkeeping practices and whether alternative identification numbers might not be developed.

So, in one sense, it is very important to counter this belief that this is an uncontrollable process. The decision to use the SSN——

Senator MOYNIHAN. An inevitable process, as you would say.

Mr. ROTENBERG. Thank you. It could be stopped if organizations chose to stop it.

Senator MOYNIHAN. We find out who I am, according to the State of New York. Yes. That is my Social Security number on my driver's license.

Mr. ROTENBERG. It is?

Senator MOYNIHAN. Yes.

Mr. ROTENBERG. All right. My third recommendation, Mr. Chairman, is to propose that a study be undertaken to look specifically at the problem of how information can be transferred from individuals to institutions without allowing institutions to engage in the secondary uses, the transfers to other institutions where the privacy problems begin.

Now, there has been a great deal of research in this area in the last couple of years by a computer scientist named David Chaum.

And many computer scientists are excited by the possibly that the particular approach that he recommends will satisfy the record-keeping needs of organizations, while protecting the privacy interests of individuals.

To use an environmental analogy, this would be like designing an engine which does not generate any pollutants. And it is certainly an idea that I hope would be pursued.

I would recommend, perhaps, that a study be undertaken either by the computer science and Telecommunications Board of the National Research Council, or by the Office of Technology Assessment.

Both organizations have recently looked at related issues and I think could offer great insight in trying to solve this particular problem. So, I thank you for the opportunity to testify. We would be pleased to answer your questions.

Senator MOYNIHAN. Well, we thank you, sir, and each of you. I do not know Dr. Chaum, but I am sure, obviously, he is a person we want to attend to. The National Research Council, of course, has the Committee of National Statistics within that council that would be interested.

What did you say was their particular committee at this point?

Mr. ROTENBERG. The Computer Science and Telecommunications Board.

Senator MOYNIHAN. The Computer Science and Telecommunications Board.

Mr. ROTENBERG. In 1990 they produced a very good report on computer security called "Computers at Risk" and touched briefly on this issue that I have raised. Now I think there would be a number of people interested in pursuing it.

Senator MOYNIHAN. Well, yes. Some graduate students at Cornell, I would expect, who seem to be hacking their way into networks in Australia. You want to give those fellows tenure. All right.

We have a problem here. We have been prepared to see the Social Security number used for whatever purposes individuals thought best, but, mind you, when hospitals start giving Social Security numbers to individual babies—well, the hospital does not; the Social Security Administration does—it is not something the new parent is likely to think much about. You know, records are records.

Keeping them, having blocks, and having fire walls between their uses is obviously not just a good idea, but it increasingly requires technology, does it not? I mean, if you do not work at it, things you do not like will happen because you cannot control them. Is that not correct?

Mr. HALPERIN. May I comment on that, Mr. Chairman.

Senator MOYNIHAN. Mr. Halperin.

Mr. HALPERIN. Mr. Chairman, I have discovered that sometimes quoting Supreme Court Justices is not as effective as quoting either Casey Stangle or Yogi Berra. And I think——

Senator MOYNIHAN. Well, we have heard Justice Douglas. Let us hear Yogi Berra.

Mr. HALPERIN. Yogi Berra was told that Dublin had elected a Jewish mayor, and he thought about it for a few minutes and said, "Only in America." And we tend to think of the United States as being far ahead on issues of protection if individual rights of various kinds, but it is not true in the privacy area.

One of the things that Janlori Goldman is working on for us is what we are going to need to do to ensure the protection of government data to conform to the standards of the European community so that, as Europe 1992 comes into effect, we will be able to exchange data with the European community.

And what we have discovered is that it is not a matter of devising new technology, although that may be helpful, it is a matter of the will and the political requirement to meet the standards that the Europeans have already adopted in the protection of this data.

So, just a mandate that government data be protected with the same concern for privacy as exists in the European community would produce substantial improvements without any new data or new thinking through about how to do these things.

Senator MOYNIHAN. Well, that is a pretty serious thought. We have an ambassador to the EC in Brussels. I think this committee should get in touch with him and say, what are those standards? If the Europeans have standards that are stricter than ours, we ought to know about that.

You always learn something on any subject I can think of by asking, what do the Canadians do? You always learn something. Sometimes it is better, sometimes it is worse, but it is always a little different. They have a Privacy Commissioner and he thinks about these things. Mr. Hendricks.

Mr. HENDRICKS. Well, I am glad that Mr. Halperin raised this issue, because, so far, the administration would benefit greatly from any advice you could give them. They have not taken a pro-privacy stance.

They have an incredible opportunity to become a leader on this issue of the EC directive. If we would do some domestic work here and raise our standards, we could turn around and help them improve some areas that we are stronger in, like the Freedom of Information Act.

But, unfortunately, we are playing the spoiler in this issue, and we are sort of throwing mud at the efforts of the EC to establish worldwide privacy standards, and I think that is not generating good will over there. Any input from Congress would go a long way toward the United States rethinking its policy.

Senator MOYNIHAN. That is very useful. Also, to point out that it is not always one way or the other. The Freedom of Information Act in the United States is probably the most open statute of its kind in the world, I would think, of a country with enough information to have the question to arise.

In the Official Secrets Act in Great Britain, you can go to jail a few years ago for reporting the number of cups of tea that are drunk in the Treasury Department cafeteria. It was pre-World War I. It was not a Cold War phenomenon at all.

Mr. HENDRICKS. I would like to turn the tables on them that way. The purpose of the EC directive is to increase the free flow of information; the idea that we cannot let personal information go to a country where there is not adequate privacy protection.

Just like a doctor and a patient have a confidential privilege so the patient can tell everything, the privacy privilege is to increase the free flow of information. The EC directive has the same purpose. So, we are in danger of suffering cut-offs of information for having inadequate privacy law which, again, goes to the fact that this has been successful——

Senator MOYNIHAN. That is a very powerful point. And I think Mr. Halperin and Mr. Rotenberg would agree, that the purpose of privacy acts is to enable an individual to tell everything he or she has to communicate to someone who needs to know it, but then it stops there.

I mean, it goes back to the freedom of the confessional in the medieval church, and it has been passed over to our statute. A lawyer may be told things that he does not have to divulge, and that enables your lawyer to do right by you.

I am going to find out about the EC directive and we will——

Mr. HALPERIN. We would be happy to submit some information to you.

Senator MOYNIHAN. Will you do that?

Mr. HALPERIN. Yes.

Senator MOYNIHAN. Good. And then we will be happy to advise our ambassador in Brussels to say, why do you not have a Freedom of Information Act? In the meantime, the need for the confidentiality of Social Security is clear. It also should be clear that individuals can get that information about themselves any time they want it.

I remain convinced that a counterfeit-proof card is an aspect of civil liberties, as well. I mean, I think that Hispanic American looking for a job in southern California ought to have a card that you can just put through an electronic slot and it says, "yes."

Mr. HALPERIN. Mr. Chairman, may I comment on that?

Senator MOYNIHAN. Yes.

Mr. HALPERIN. Because I think we do have a serious disagreement about that, and one that we share with the Hispanic community.

They believe that what would happen is that only Hispanics would be asked for that card, and that you would have a two-tiered system of discrimination and that the unreliability of the data in the immigration system and in the Social Security system would lead to endless difficulties for the Hispanic community.

So, they believe, in fact, and we believe, that it would produce a greater degree of discrimination.

Also, as you know, it is one thing to produce a non-counterfeit Social Security card, which is enormously expensive, as you know. To convert every card to a non-counterfeit card would be an enormous and very expensive undertaking.

But the other problem, as you know, is the documents you need to get a Social Security card. And as long as it is——

Senator MOYNIHAN. Yes. We will not disagree. It has been too agreeable a hearing. But the cost comes to about 2 cents per card. There are variations on it, but it is not such that American Express does not manage to send you a new one every year.

And we can talk about that. But we have moved the subject from southern California to Astoria. I mean, everyone with an Irish accent is under the presumption of maybe it is not quite kosher, and so, we should keep that in sight, as well.

Mr. ROTENBERG. Mr. Chairman.

Senator MOYNIHAN. Sir.

Mr. ROTENBERG. If I could add just a point to this. I took it from your earlier comments about the creation of a Social Security system in the 1930's, that maybe some of the concerns then about a national ID card may have been ill-founded or based on the particular concerns about Nazi Germany.

But, I should say, over the last couple of years, our organization has looked increasingly at the development of computerized record-keeping systems in Third World countries. And we are, frankly, quite concerned about the shape that these national ID cards do take.

A system that was developed in Thailand, for example, a couple of years ago, which contains on the card the person's party affiliation and type of employment.

In Malaysia, for example, people carry cards that are color-identified, based not simply on citizenship status, but also as to whether there is any prior criminal record.

And we begin to see a world that looks something like Aldus Hucksley's "A Brave New World" in which people are fairly quickly categorized and a new caste system is created. So, I share very much Morton Halperin's concerns about the creation of that card.

Senator MOYNIHAN. We do not have any disagreement on that at all. The internal passports that the Soviet Union had showed what your religion was, et cetera, et cetera.

That is not the case with our Social Security numbers; it simply says your name and your number. We want to be concern that that information is kept confidential. We also want to be concerned that the information is accurate.

I wish people would get more in the habit of asking for their records just to make sure the records are right.

We have, in statute, a provision that over this decade will require the Social Security Administration to mail out once a year your Social Security statement so you can look at it. The largest expense involved will be the stamp. The information is there, and it can be gotten.

We have more work to do, obviously. We thank you very much. I am going to get that directive from the EC from you. Any further thoughts on the Privacy Act we would be very much appreciative of.

I think I hear you say that this subcommittee, which has responsibility for Social Security, ought to be more concerned about what other committees around Capitol Hill are using and directing that

that number be used for some reason that is no way involved with Social Security itself.

I can see us doing that, and I think we ought to do it, and it is time we did it. And for all that, we thank you, gentlemen. We thank you for the work you do.

This is not the end of the subject; it is obviously the beginning, and a good one. We want to thank Margaret Malone, and Ed Lopez, and all of the staff who have put this together. And I see we have work to do, and that is what we are here for. Thank you very much.

Mr. HALPERIN. Thank you, Mr. Chairman.

Mr. HENDRICKS. Thank you.

Mr. ROTENBERG. Thank you.

[Whereupon, the hearing was concluded at 11:45 a.m.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED

PREPARED STATEMENT OF LOUIS D. ENOFF

Mr. Chairman and Members of the Subcommittee: I am happy to be here today on behalf of Commissioner King to respond to your request to discuss protection of personal information in Social Security Administration (SSA) files.

Let me say at the outset that we are very concerned about the recent indictment of several SSA field office employees for selling employment and earnings information. There is simply no excuse for such behavior, and no place for it at SSA.

Although we firmly believe in the honesty and integrity of our workforce as a whole, we have state-of-the-art systems security safeguards in place to deter employees who could be tempted to misuse their position of public trust. These safeguards successfully identified the misuse of Agency systems files, and enabled us to refer the case to the Office of the Inspector General for investigation.

PROTECTION OF INFORMATION IN SSA RECORDS

SSA always has taken its responsibility to protect the privacy of personal information in Agency files most seriously. When the Social Security program began, people were concerned that information they provided to Social Security could be misused. To allay these fears, the Social Security Board announced, in November 1936, that the information required of any worker would be regarded as confidential and would be used only for Social Security purposes.

In its very first regulation, issued in 1937, the Social Security Board formalized its pledge that information would be kept confidential. This pledge of confidentiality has been an important factor in the cooperation which employers and employees have shown over the years in providing required information.

Until relatively recently, the confidentiality of SSA information was protected not only by SSA's commitment to safeguard it, but also by the physical inaccessibility of the information, which generally was stored in paper folders housed in huge record centers. Of course, the difficulty of retrieving information under this system also meant that local Social Security offices had to wait days or weeks to get the information they needed to process a claim or answer a beneficiary's questions.

Increased computerization of Social Security in the last decade has made it possible today for Social Security field employees to receive information needed to handle a claim or answer a question within seconds. While this ease of access has improved dramatically SSA's ability to serve the public, it also has made the protection of SSA information more difficult. What we have had to do, therefore, is find new ways to guard against unauthorized access to and use of SSA information.

I would like to describe briefly the major types of information SSA maintains, the risks we see of unauthorized use, and our safeguards to prevent misuse.

TYPES OF SSA INFORMATION

SSA stores three types of personal information in automated files:

- personal identifying information, such as date and place of birth and parents' names, which is collected when an individual applies for a Social Security number;
- Earnings and employer information collected from self-employed individuals' tax returns and from Forms W–2 filed by employers, including names and addresses of employers, and amounts earned each year; and
- Benefit-related data such as monthly payment amounts and current addresses for people who are receiving benefits.

RISK OF UNAUTHORIZED USE OF SSA DATA

As I mentioned earlier, the major risk of misuse of SSA information arises from the need to make all major data files as accessible as possible to SSA employees who deal with the public. Such ready access to data files is essential to provide good service. The advent of computer systems which permit access to data files in seconds without any paper trail or the involvement of any other person has increased the risk that an employee who is authorized to use the system may obtain and misuse information.

Experience has shown us that two types of computer requests or "queries" of data files are most susceptible to misuse by employees and must be treated as especially sensitive. These are:

- The "Alpha-Index" query, which is used to identify the Social Security number assigned to a name. The SSN provides access to all information about an individual in other SSA files; and
- The Detailed Earnings query (DEQY), which provides employer names and addresses and the amounts earned by year.

In the cases involved in the indictments publicized in December 1991, four SSA employees in different parts of the country were allegedly approached by information brokers—people who buy and sell personal information from the records of Federal, State, and local agencies—and offered money to provide employment and earnings information. Such information is in demand both to verify credit applications and to locate individuals by obtaining the names and addresses of their employers.

SAFEGUARDS AGAINST MISUSE

During the planning for automation of our data files, SSA was extremely concerned about the increased risk of misuse of data that such automation would bring. To find ways to minimize that risk, we visited major banks and insurance companies to see how they protected data in their automated systems.

We learned a great deal about techniques that have been developed in the private sector to safeguard information in automated files, and we built the best of those safeguards into our new systems when they were implemented in the mid- and late 1980's.

The first type of safeguard of automated files is to prevent access by people *not* authorized to use the information in a file. The standard way this is done is to require a personal Identification Number, or PIN, and a PASSWORD in order to get into the system.

SSA assigns PINs to employees on a "need to know" basis that is tied to the type of job the employee performs. In addition, even the employees who can enter the automated system do not have access to all the files that SSA maintains. We use a commercial software package called "Top Secret" to control access to each file and allow employees to access only the information they need to do their particular type of job. This widely used software was evaluated by the National Security Agency and found to be appropriate for SSA systems security purposes.

These safeguards to control access to SSA files have proven extremely dependable. However, in any automated system that large numbers of employees must use, there is an unavoidable vulnerability to misuse. As the experience of the national intelligence agencies, the Federal Bureau of investigation, the Internal Revenue Service, and other agencies has shown, some people authorized to use any large system may respond to bribes to misuse information.

To deal with this fact of life in protecting sensitive systems, SSA has built a second safeguard into our system—the capability to monitor access to sensitive files. Each time one of these sensitive files is accessed, an audit trail is automatically established as a by-product of the transaction. The audit trail capability is critical for three reasons. First, it discourages misuse because employees know their access to sensitive files is monitored. Second, it triggers reviews of unusual patterns of access to sensitive files. And third, it enables investigators to trace use of the system to confirm suspected misuse, and to gather the evidence needed for prosecution. It was this audit trail capacity that made the recent indictments possible.

The audit trail capability is used by SSA's systems security officers in Baltimore and in our regional offices to monitor access to sensitive files on both a random basis and on a targeted basis involving a specific office, a specific employee, or an individual Social Security number.

These systems security officers are the third safeguard in SSA's systems. Security officers develop and enforce SSA's overall systems security policy and guidelines, monitor adherence to security plans and initiatives, and make sure that the automated security safeguards are working properly. Regional security officers also en-

sure that SSA field offices are following nationally mandated security controls and provide assistance to the employee in each field office who is responsible for systems security.

The fourth type of systems security safeguard we use is local field management reviews of actions processed in their offices (such as requests for Social Security cards) to ensure that they are legitimate. This can be done either by examining available documentation or by recontacting the individual reporting an event. Some of these local reviews are mandated by national SSA policy, while others may be performed randomly at the manager's discretion to deter and detect fraud. Local security officers and other management officials are taught to watch for any incident or pattern of behavior which is out of the ordinary and may indicate that an employee is involved in the sale or misuse of information. For example, if an employee who does not routinely handle earnings inquiries begins to request an unusual number of DEQYs, the supervisor or local security officer will investigate further to determine if there is any indication of possible misuse. If there is, the regional systems security officer and the Office of the Inspector General are alerted. Only the Inspector General is authorized to conduct investigations of illegal activities.

The final safeguard to prevent misuse of SSA information is careful training of employees about the confidential nature of the personal information in SSA's files and the penalties for misuse of that information. Our security personnel detail for employees the proper use of the information that can be obtained through on-line queries. All of our employees who have on-line access to earnings and SSN files receive periodic training about the restrictions that apply to the use of this information. Also, each person who is issued a PIN certifies, in writing, that he or she understands and will comply with SSA's disclosure policy.

Our security personnel also train local managers to conduct their own reviews of the use of sensitive queries in their offices and to detect employee abuse of the system.

POSSIBLE ACTIONS TO IMPROVE SECURITY

We are now exploring ways we can improve our safeguards without decreasing the level of public service we provide. These possibilities include:

- Seeking legislation for increasing the monetary penalties for misuse so that they clearly outweigh any possible profit from the sale of information;
- Issuing special bulletins to employees on the importance of guarding the privacy of SSA information and the severe penalties that apply; and
- Making SSA employees aware of the convictions and penalties imposed on those found guilty of misusing information. As the FBI's National Crime Information Center section chief recently noted, there is only one sure way to deal with people who misuse confidential information, and that is to aggressively pursue their prosecution.

As technology improves, any large organization becomes more and more vulnerable to both internal and external security breaches. Therefore, we are continually exploring additional preventive measures for maintaining systems security. In short, the focus of our efforts is to make employees aware that anyone who offers to buy information must be reported immediately and that the penalties for sale of SSA information include termination of employment and prosecution under Federal criminal law.

RESTRICTIONS ON USE OF THE SSN

You also asked that we discuss restrictions on private sector use of the SSN. As you know, Federal statutes regulate when and how Federal, State, and local governments may use the SSN. However, Federal law is silent on the various uses of the SSN in the private sector today, with one important caveat. The Internal Revenue Code requires that an individual provide his or her taxpayer identification number (TIN) to anyone who must report dividends, interest, or other taxable payments. Thus, financial institutions, insurance companies, and some other private sector entities must request the TIN of their clients.

Most complaints about use of the SSN in the private sector appear to involve consumer credit bureaus. Generally, the complaint is that credit bureaus have confused names or SSNs and reported the wrong credit information for an individual.

The privacy protection Study Commission, created by the privacy Act of 1974, was directed to study the use of the SSN in our society. The Commission concluded that a unique identifier in large systems of records is essential. The Commission stated in its 1977 report that it did not believe legal restrictions on the collection or use

of the SSN by private organizations were appropriate at that time, but recognized that such use could be a continuing concern.

CONCLUSION

Mr. Chairman, SSA always has made confidentiality of personal information in our files a cornerstone of our policy. The agency mission, however, is to serve the public as quickly and effectively as possible. This requires that thousands of SSA employees have access to the personal information in our files.

Thus, SSA, like all organizations with confidential information of value to outsiders, is vulnerable to misuse of that information by its employees. To deal with this vulnerability, we have identified the information in our files that is valuable to outsiders and put in place sophisticated safeguards to prevent misuse of that sensitive data.

Prepared Statement of Morton H. Halperin

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to testify before you today on behalf of the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization of more than 275,000 members devoted to protecting the Bill of Rights. The ACLU Project on Privacy and Technology was created in 1984 to examine the impact of emerging technologies on individual privacy rights and other civil liberties.

The ACLU is very concerned about the recent arrests of government agency employees nationwide for selling confidential information held in government records. These arrests bring to light a growing problem in the United States -- the increasing demand for detailed, sensitive information by employers, insurance companies and others, coupled with the ease with which "insiders" can disclose and exchange computerized government records, has created a booming blackmarket in confidential information.

Our testimony today addresses three issues: 1) the unauthorized disclosure of personal information by government employees; 2) the disclosure of personal information held by the private sector; and 3) the role of the Social Security Number (SSN) in the creation and dissemination of personal files by both the government and the private sector. We conclude our statement with a set of privacy proposals for tighter, more effective controls on personal information held by the public and private sector.

I. OVERVIEW

People disclose a tremendous amount of personal information in exchange for receiving benefits and services from the government and the private sector. In most cases, people lose control over how the information is used and by whom. This loss of control is exacerbated as government agencies and private institutions escalate the collection and exchange of personal information. Advanced information technology now gives institutions, both public and private, the power to nearly instantly exchange, compare, verify, profile, and most importantly, link information. In a 1986 report on electronic records and individual privacy, the Office of Technology Assessment (OTA) concluded that a de facto national database already exists on U.S. citizens.

The right to privacy protection for personal information has grown increasingly vulnerable with the growth of advanced information technology. New technologies enable people to receive and exchange ideas differently than they did at the time the Bill of Rights was drafted. The new technologies not only foster more intrusive data collection, but make possible increased demands for personal, sensitive information. The computer now makes possible the instant assembly of this information. Personal papers once stored in our homes are now held by others with whom we do business.

The ACLU believes, as does the majority of the American public, that privacy is an enduring and cherished value and that legislation is necessary to protect personal, sensitive information. People care deeply about their privacy, and cherish the ability to control personal information. Even if they have done nothing wrong, or have nothing to hide, most people are offended if they are denied the ability to keep certain personal

information confidential. Crucial to one's sense of self is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose.

A June, 1990 survey by Louis Harris & Associates, Consumers in the Information Age, found a growing public demand for privacy legislation, documenting that an overwhelming majority of people believe that their right to privacy is in jeopardy. The survey also found that 79% of the American public stated that if the Declaration of Independence were rewritten today, they would add privacy to the list of "life, liberty and the pursuit of happiness" as a fundamental right. In fact, the Bush Administration, through its Office of Special Advisor for Consumer Affairs has made the protection of information privacy a priority issue.

In 1971, Alan Westin, in his book Data Banks in a Free Society, warned: "We have seen that most large-scale record systems in this country are not yet operating with rules about privacy, confidentiality, and due process that reflect the updated constitutional ideals and new social values that have been developing over the past decade." Although substantial progress has been made since 1971, we still have a long way to go.

II. CONGRESSIONAL RESPONSE AND THE PRIVACY ACT OF 1974

Congress has struggled with the problems posed by increasing information collection and use, and the development of new information technologies that are transforming the way institutions handle information. In the 1960's and early 1970's, Congress held a series of hearings on computers, privacy and the protection of personal information.[1] Throughout most of the 1960's, Congress considered a proposal to create a centralized national data center on all U.S. citizens containing information such as Social Security numbers, income and census data. Backers of the proposal argued that the center was necessary to serve the needs of the "welfare state." After years of hearings, studies, and debates, the national data center was overwhelmingly condemned as "Big Brother" government, and a threat to individual autonomy, dignity, and liberty.

By 1973, the Watergate scandal contributed to what had then become a national crisis of faith in government institutions and a heightened sensitivity to the unfettered ability of the government to intrude into the personal affairs of its citizens. The public reacted with increasing alarm over the unhampered collection and use of personal records by the government:

> Accelerated data sharing of such personally identifiable information among increasing numbers of federal agencies through sophisticated automated systems, coupled with the recent disclosures of serious abuses of governmental authority represented by the collection of personal dossiers, illegal wiretapping, surveillance of innocent

---

[1] The Computer and Invasion of Privacy: Hearings Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Government Operations, Cong., 2nd Sess. (1966); Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 92nd Cong., 1st Sess. (1971); and Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 93rd Cong., 2nd Sess. (1974).

> citizens, misuse of tax data, and similar types of abuses, have helped to create a growing distrust or even fear of their government in the minds of millions of Americans.[2]

An advisory committee within the Department of Health, Education and Welfare (HEW) published a report in 1971 entitled Records, Computers and the Rights of Citizens, which proposed a Code of Fair Information Practices to be used by federal agencies. The basic principles of the Code are: 1) there must be no personal data record-keeping systems whose very existence is secret; 2) an individual must be able to find out what information is in his or her records and how the information is being used; 3) an individual must have the right to correct information in his or her records; 4) any organization creating, maintaining, using or disseminating personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and 5) an individual must have the ability to prevent information about him or her that was obtained for one purpose from being used for another purpose without consent.

The Code became legally binding on agencies when it was incorporated into the Privacy Act of 1974. In passing the Act, Congress explicitly recognized that:

> 1) The privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information by Federal agencies;
>
> 2) The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;
>
> 3) The opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
>
> 4) The right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
>
> 5) In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies.[3]

In introducing the Senate version of the Bill, Senator Sam Ervin (D-NC) said: "[T]he appetite of government and private organizations for information about individuals threatens to usurp the right to privacy which I have long felt to be among the most basic of our civil liberties as a free people...[T]here must

---

[3] Privacy Act of 1974, 5 U.S.C. 552a (2)(a).

[2] H.R. Rep. No. 1416, 93rd Cong., 2d Sess. 3 (1974), reprinted in, Source Book, at 296.

be limits upon what the government can know about each of its citizens."

The Act establishes a right of privacy in personal information held by federal agencies. With certain exceptions, the Act prohibits government agencies from disclosing information collected for one purpose for a different purpose without the individual's consent. Under the Act, citizens have a right of access to their records and the opportunity to amend their records upon showing that they are not accurate, relevant, timely, or complete. The Act also limits the use of the Social Security number for identification purposes, unless otherwise authorized by law, and prohibits the government from collecting information on the political activities of citizens. Individuals may sue for injunctive relief to enforce some of the Act's provisions, and damages may be awarded by proving that harm occurred as the result of a willful or intentional agency violation of privacy.

Despite the good intentions and clear objectives of its drafters, the Privacy Act has fallen far short of achieving most of its laudable goals, at best serving as a procedural hoop-jump for federal agencies. The Act's potential impact has been watered down, due in part flaws in the Act itself, administrative interpretation, and lack of enforcement. The basic principles of the Privacy Act have failed to limit significantly the government's use of personal information. In fact, agencies have escalated the collection and dissemination of personal information. The Act is no longer viewed as an effective barrier to the disclosure of confidential information.

In 1977, the Privacy Protection Study Commission, created by the Privacy Act to study additional privacy issues and recommend future legislation, issued its report Personal Privacy in an Information Age. The report recommended that the Privacy Act be more vigorously enforced, and suggested a number of ways to make the Act more effective. The Commission found that the Act "has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect."

The Office of Management and Budget (OMB) is responsible for oversight and guidance responsibilities of the Privacy Act. However, as the Privacy Commission found, "neither OMB nor any of the other agencies...have played an aggressive role in making sure that the agencies are equipped to comply with the Act and are, in fact, doing so." By the early 1980's, a consensus was developing that OMB had "virtually abdicated responsibility" for enforcing and overseeing the Act.[4] There is no better proof of the Act's failure than the sweeping arrests at the end of last year of government employees for selling confidential information protected by the Act.

These recent reports of the sale of personal information held by government agencies illustrate the widespread and troubling problem of unauthorized disclosure of records by "insiders" -- people who have authorized access to personal information in government record systems, such as police officers and social security clerks.

---

[4] Oversight of the Privacy Act of 1974: Hearings before a Subcomm. of the House Comm. on Government Operations, 98th Cong., 1st Sess. 259 (1983) (statement of John Shattuck). See also, House Comm. on Government Operations, Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and the Congress, H.R. Rep. No. 455, 98th Cong., 1st Sess. (1983).

In December, 1991, the FBI arrested eighteen people on charges of selling confidential information held in government records systems such as income tax, work history, and criminal history records. The FBI claims that employees from the Internal Revenue Service, the Social Security Administration, law enforcement agencies and others illegally sold confidential information to private investigators, insurance companies and information brokers. One information broker, National Electronic Tracking (NET), advertised in brochures to private investigators promises to process requests for "confidential data .... 24 hours a day, 7 days a week." The FBI alleges that companies such as NET purchased earnings histories, criminal history records, tax records and other confidential records from government employees and then sold the information for a substantial profit.

FBI Director William Sessions objected strongly to the unauthorized disclosures: "Every person in this country has the right to expect that personal information will only be released for legitimate purposes. The FBI is deeply concerned about the integrity of this information and will continue to vigorously investigate any individuals who compromise the public's right to privacy." (Washington Times, 12/19/91).

Unauthorized disclosures of confidential personal information held by government agencies are not new. The confidentiality of Census Bureau information was violated during World War II to help the War Department locate Japanese-Americans so they could be forcibly moved to internment camps. And, during the Watergate years there were illegal disclosures and uses of Internal Revenue Service documents and other government records for political purposes. In addition, during the Vietnam War, the FBI secretly operated the "Stop Index" by using its computerized National Crime Information Center (NCIC) to track and monitor the activities of people opposed to the United State's involvement in the war.

As previously discussed, the federal Privacy Act prohibits most of these disclosures, but the law is not effectively enforced. For instance, the Act does provide for a private right of action for disclosures in violation of the law, but the law has been interpreted to be limited to actions against agencies of the U.S. government. Thus, the Privacy Act does not provide a right of action against state agencies or private entities, many of whom were the subjects of the recent arrests. The Act does provide for a misdemeanor criminal penalty and a maximum $5,000 fine against an agency employee who violates the law. In addition, the same criminal penalty may be applied to "any person who knowingly obtains a record under false pretenses." (552a i (1)-(3)).

Further, it is extremely difficult for people harmed by violations of the Act to bring suit under the law. The Act's lack of both a broad injunctive relief and liquidated damages provision hamper meaningful litigation under the Act. Privacy violations often result in intangible harm to individuals, making it very difficult to prove actual damages as required by the Act.

The ACLU believes that the Privacy Act should be amended to strengthen and broaden the civil and criminal penalties provisions. First, civil and criminal penalties should be applied broadly to any person who has authorized access to records covered by the Privacy Act. Second, both the civil and criminal penalties in the Act should be increased to deter future unauthorized disclosures. Third, agencies should be required under the Act to put in place strict security measures to safeguard records, such as audit trails and passcodes for logging on to systems. In general, individual agencies, the Office of

Management and Budget, and appropriate congressional oversight committees should more strenuously oversee agency compliance with the Privacy Act.

A separate, but equally important issue, is the authorized disclosure of personal information held by the government, some of which we believe should be restricted. We believe the Privacy Act should be amended to narrow certain authorized disclosures under the law. The Act's central rule that there be no disclosure of a record in a system of records except pursuant to a written request by, or with the prior written consent of the subject is undermined substantially by the twelve exceptions to the rule. The Act's most insidious loophole is the "routine use" exception, which allows disclosures of a record for a purpose "compatible with the purpose for which it was collected." (552a (b)(3). This exception has been interpreted so broadly as to undermine the central purpose of the law.

In this context, the ACLU is extremely concerned about the authorized disclosures of criminal history records by the FBI. Nearly half of all requests to the Bureau for criminal history records are from non-law enforcement entities, such as employers and licensing boards. Recently, the FBI was successful in its efforts to abolish the "one year rule," the federal regulation barring dissemination to non-law enforcement requesters of arrests records over one year old that did not contain dispositions . The ACLU vigorously opposed repealing the rule on the grounds that nearly half of the FBI's records lack dispositions due to poor reporting by state agencies. The release of incomplete records will lead to discrimination against minorities in employment (minorities are arrested four times more frequently than whites, and a large percentage of those arrests do not end in conviction). We urge Congress to enact legislation reinstating the "one-year rule."

III. PERSONAL INFORMATION HELD BY THE PRIVATE SECTOR

Congress has responded to the pressing need to protect personal information held by the private sector. In the last twenty years, Congress has made substantial progress in the area of federal information privacy legislation, regulating government and private access to privately-held personal information. Most of these laws incorporate the central principle of the Privacy Act of 1974 -- information collected for one purpose may not be used for a different purpose without the individual's consent.

-- In 1970, Congress passed the Fair Credit Reporting Act to regulate the credit reporting industry's use of personal information;

-- In 1974, the Family Educational Rights and Privacy Act was passed, limiting disclosure of educational records to third parties;

-- In 1978, Congress passed the Right to Financial Privacy Act, restricting access to personal information held b financial institutions;

-- In 1980, Congress passed the Privacy Protection Act to prohibit the government from searching press offices without a warrant if no one in the office is suspected of committing a crime;

-- In 1982, Congress passed the Debt Collection Act requiring federal agencies to provide individuals with due

process protections before an individual's federal debt information may be referred to a private credit bureau;

-- In 1984, Congress enacted the Cable Privacy Protection Act to safeguard the confidentiality of interactive cable subscription records;

-- In 1986, the Electronic Communications Privacy Act (ECPA) was passed, amending the Wiretap Law to cover the interception of non-aural communications; and

-- In 1988, the Video Privacy Protection Act was enacted, in response to the disclosure of Judge Robert Bork's video rental list during his Senate confirmation hearings to the U.S. Supreme Court.

The ACLU is currently supporting efforts to update and strengthen a number of existing privacy laws, including the Fair Credit Reporting Act and the Electronic Communications Privacy Act. Bills to amend both of these laws are pending in the House and the Senate. In addition, we believe legislation is necessary to create legally enforceable protections for medical, insurance and personnel records.

Further, the ACLU has long opposed the growing use of the Social Security number and recent congressional proposals for a national identification card as significant threats to individual privacy and other civil liberties.

IV. THE SOCIAL SECURITY NUMBER

In both the public and the private sector, the Social Security number (SSN) has become a "de facto national identifier." Many believe that the SSN is the key used to open the door to personal information held in databases. Clearly, the use of the SSN as a unique identifier may make the retrieval of information easier, but limiting the number's use is only one step needed to create greater protections on the misuse of personal information. For instance, many large organizations file and retrieve records using a variety of identification devices, including fingerprints, names, birthdates, and zipcodes.

Over the past fifty years, the SSN has evolved from a single-use identifier to the identification number of choice for both the public and private sector. In this computer-driven era where information is often connected to a single identifier, such as the SSN, and entered into massive databases, it is possible to instantly exchange, compare, verify and link information in separate databases, often without the knowledge and consent of the person divulging the information. As the recent arrests of government employees illustrate, such a storehouse of information presents a very real potential for abuse.

Attempts to reverse the trend towards turning the SSN into a de facto national identification number have been largely unsuccessful. And, in recent years there have been proposals to establish a national identification card in response to concerns over illegal immigration and gun control. (See Hearing, House Ways and Mean Subcommittee on Social Security, 2/28/91, testimony of ACLU).

People are overwhelmed by the number of circumstances in which the SSN is requested, and people are often not informed about how the number can be used as the key to link information in other databases. For many Americans, it is troubling to know that the government has easy access to a wide range of information about them, can track their movements, and put together a "womb-to-tomb dossier" at the push of button. In

particular, political activists and people receiving government benefits generally come into more direct contact with the government than the average citizen and thus have more to fear from the creation of a national ID card and the compiling of dossiers. In his book Databanks in a Free Society, Alan Westin wrote that "many dissenting and minority groups in [American] society...view the establishment of such an identifier...as a giant step toward tightening government control over the citizen for repressive purposes." Large-scale information systems, even those created for a limited purpose, inevitably take on a life of their own -- the temptation to use the information for other purposes is irresistible.

The SSN was created in 1935 solely for the purpose of tracking contributions to the social security fund. The Social Security Act required that the Social Security Administration keep records on millions of workers for the rest of their lives. Workers covered by the Social Security program were issued an account number, which they were then required to report to employers. In turn, employers then reported to the IRS information on wages paid and taxes withheld from their employees.

In a move towards efficient recordkeeping, President Roosevelt issued Executive Order 9397 in 1943, which encouraged federal agencies to use the SSN when establishing a "new system of permanent account numbers pertaining to individual persons." In 1961, the Civil Service Commission began using the number to identify all federal employees. The following year the IRS required the number on all individual tax returns. Widespread use of the number began in the mid-1960's, however, when the development of the computer coincided with burgeoning public assistance programs.

Over the next decade, the number's uses by the government and the private sector expanded dramatically. As the demand for the number grew, so did concern over its abuse. In 1971, a Social Security Administration Task Force issued a report decrying the run-away use of the SSN for identification purposes:

> The increasing universality of the social security number in computer data collection and exchange represents both substantial benefits and potential dangers to society; [a] national policy on computer data exchange and personal identification in America [is necessary], including a consideration of what safeguards are needed to protect 'individuals' rights of privacy and due process.

In 1973, HEW issued a report entitled Records, Computers and the Rights of Citizens, warning that the creation of a standard universal identifier would lead to a national dossier system that could track people for a lifetime. The HEW report strongly opposed the implementation of a national identifier because an "uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems" had the potential to lead to invasions of privacy.

Congress responded by limiting the use of the SSN in a provision of the Privacy Act of 1974. The Act prohibits a local, state or federal agency from requiring an individual's Social Security number as a condition of receiving services or benefits, unless this is authorized by law.[5] Congress feared that if the

---

[5] 5 U.S.C. § 552a (1974).

"use of the SSN as an identifier continues to expand, the incentives to link records and broaden access are likely to increase." The Senate Committee report described the growing use of the number as "one of the most serious manifestations of privacy concerns in the nation," including the risk that "the number may become a means of violating civil liberties by easing the way for intelligence and surveillance uses of the number for indexing or locating the person." Congress was concerned that the number was on its way to becoming a national identifier, and would be used as the uniform identifier in linking separate records systems.

In its 1977 report, the Privacy Protection Study Commission found widespread opposition to the use of the SSN as a national identifier because individuals:

> resent being identified by a number rather than a name;
>
> fear that if several organizations possess an individual's SSN the ability with which those organizations can exchange information about the individual will be greatly facilitated, and are concerned that if the SSN is used to facilitate unconstrained exchanges of information about people, dossiers about individuals may be created that will follow them throughout life.

Seeing "a clear danger that a government record system, such as that maintained by the Social Security Administration or the Internal Revenue Service, will become a de facto central population register," the Commission's final recommendation was that the federal government "act positively to halt the incremental drift toward creation of a standard universal label and central population register until laws and policies regarding the use of records about individuals are developed and shown to be effective.

Unfortunately, despite the fact that Congress has specifically rejected the use of the SSN as a national identifier, it has played a large role in the number's expansion, authorizing and requiring it for many government programs. For example, the Tax Reform Act of 1988 requires that children claimed as dependents on tax returns must have an SSN. In addition, Congress authorized states to require the number as the identifier on drivers' licenses and the SSN is required to apply for most government benefits and programs. The number is also requested, but not always required, for a wide variety of commercial transactions, including applying for credit, employment, insurance, as identification on a check and even to enroll in college.[6] The overall result has been, as the Congressional Office of Technology Assessment (OTA) concluded in 1986 that the SSN had become a "de facto national identifier."

This unintended result occurred for a variety of reasons but it is important to note here that although Congress has consistently opposed the creation of a national ID card and

---

[6] In 1989, the New York legislature passed a law prohibiting merchants from asking customers for the social security number and other personal information when using a credit card. The law is intended to restrict the collection and sale of personal information for marketing purposes.

sought to slow the growing use of the SSN. In fact, Congress has recognized abuses of the SSN. The Social Security Administration (SSA) used to be in the business of selling SSN verifications to the private sector until Congress put a stop to the activity. Three years ago, it was discovered that the SSA had been using its massive data files to verify SSNs for commercial purposes. Following press reports, the SSA Commissioner announced in April, 1989 that the agency decided not to continue processing magnetic tapes containing 140 million names and SSNs submitted by TRW Credit Data, a credit reporting company.[7]

At a Senate hearing on the matter, Senator David Pryor expressed outrage at SSA's earlier verifications for industry, claiming the agency had violated peoples' right of privacy. Pryor chastised SSA's Commissioner: "As far as I'm concerned, this is as far away from the mission of the S.S.A. as anything I've ever heard of."[8] Senator Pryor then commended SSA on its decision to halt verification of SSNs for businesses:

> "I am glad that Commissioner Hardy has taken this path and seen fit to preserve the confidentiality of the Social Security files. Unfortunately,...this action comes too late to protect some 150,000 people whose files were violated during a test run for TRW and for more than three million people on whom verifications were conducted for Citibank and other firms in past years."[9]

The private sector's use of the SSN to access information about individuals has evolved to a point never envisioned by its creators. For example, in a 1990 advertising brochure, TRW Credit Data, which holds itself out as the nation's largest provider of consumer credit information and claims to maintain information on nearly 170 million consumers nationwide, advertises a service called Social Search:

> In pursuit of those who have disappeared - former customers, college alumni or missing shareholders - TRW brings you Social Search: A state-of-the-art locating tool that puts our expansive databases to work for you . . . All you need are the Social Security numbers of those you're attempting to locate and you can reach those hard-to-find individuals who may have moved or changed their names.

Despite its burgeoning use, the SSN is a notoriously unreliable identifier. Of the over 210 million SSNs in use today, about 75 percent were issued before evidence of age, identity, and citizenship or alien status were required. Only 76 million of the initial and replacement social security cards have been issued using the new counterfeit and tamper-resistant paper, so that most cards in use are easy to alter or forge. And, there is no method to positively assure that any person presenting a social security card is the person to whom it was issued since the card contains only a name, SSN, and signature.

---

7 Washington Post, April 14, 1989 at A-10.

8 New York Times, April 15, 1990, at 1.

9 Id.

V. RECOMMENDATIONS

The ACLU recommends that Congress take the following actions:

1) amend the Privacy Act of 1974 to strengthen the disclosure standards, and increase and broaden the civil and criminal penalties provisions;

2) amend the Privacy Act to include a prohibition on the creation of a national identification card;

3) strengthen and update existing privacy protection statutes governing the private sector, including the Fair Credit Reporting Act and the Right to Financial Privacy Act, to give people greater control over how personal information is used; and

4) to enact legislation to fill significant gaps in privacy law to protect medical, insurance and personnel records.

VI. CONCLUSION

The ACLU commends this Subcommittee for holding this important hearing. We look forward to working with you in the coming months.

PREPARED STATEMENT OF EVAN D. HENDRICKS

Mr. Chairman, I'd like to thank you for the invitation to testify before the subcommittee. Your hearing provides an important opportunity to focus attention on threats to privacy posed by the misuse of personal data and the ill-conceived expansion of uses of the Social Security number in the public and private sectors.

My name is Evan Hendricks. I'm editor/publisher of PRIVACY TIMES, a biweekly, Washington-based newsletter that reports on legal, policy, industry and consumer news in the fields of privacy and freedom of information. I started PRIVACY TIMES eleven years ago. I have been reporting on privacy and FOIA issues for 14 years. I am author of the book Your Right To Privacy (SIUP-1990).

I am also Chairman of the U.S. Privacy Council, an organization consisting of individuals who work on a variety of fronts to foster better practices and policies in relation to the uses of personal information.

In this written testimony, I will explore:

1) The significance of the recent Federal investigation of the allegedly illegal sales of personal data.

2) The reasons why privacy protections in the U.S. are generally weak, inadequate and outdated.

3) The evolution of the SSN as the individual identifier of choice for government agencies and private sector organizations.

4) Concrete proposals to limit uses of the SSN and strengthen protections for personal privacy.

5) Immediate steps the subcommittee can take towards the establishment of a comprehensive policy on use of the SSN.

The "Information Broker" Case

On December 18, 1991, Michael Chertoff and Robert Genzman, U.S. Attorneys for Newark, N.J. and Tampa, Fl., respectively, announced the indictments of eight "information brokers," three Social Security Administration employees and five other individuals in connection with the allegedly illegal sale of confidential government data stored in FBI and SSA computers.

Although no individuals have yet been convicted on any of the indictments, it appears that federal investigators uncovered a wide ring of individuals who were profiting from the sale personal data maintained in government computers that was supposed to be confidential under federal law.

This investigation represents the first major effort by authorities to crack down on the illegal sale of personal data held by the government. As a privacy advocate, I enthusiastically applaud the U.S. Attorneys and Department of Health and Human Services Inspector General agents that have worked hard over many months to halt the allegedly illegal invasions of citizens' privacy.

As U.S. Attorney Chertoff said, "Confidential government files and a U.S. citizen's right to privacy should not be sold to the highest bidder. The information that resides in government databases is not a commodity in which government employees should traffic and from which others should profit."

Unfortunately, I fear the "information broker" investigation has merely uncovered the tip of a very large and ugly iceberg. There are indications that the investigation continues expanding, as authorities learn more about those trafficking in personal data.

Moreover, the under-the-table sale of personal data traditionally has been thought of as "something that everyone knows is happening, but which nobody can prove or otherwise do anything about."

On January 3, for instance, U.S. Attorney Chertoff announced the indictment of a former chief of the IRS Criminal Investigative Division on charges that he used his position to obtain nonpublic marital records and sell them to an investigative firm run by former IRS agents.

In 1989, the IRS reported that more than 20 of its agents illegally obtained credit reports. One unnamed IRS collection employee, who apparently had a grudge against a taxpayer, obtained the taxpayer's credit report and leaked it to a state regulatory agency, hoping to get that taxpayer in trouble. Instead, the state agency, cooperating with the credit bureau and IRS managers, identified the collection employee, who was prosecuted for violations of the Fair Credit Reporting Act. (See *Privacy Times*, March 18, 1991.)

In 1982, police officers in St. Louis and private detectives the firm Fitzgerald & Dorsey pleaded guilty to criminal violations of the Privacy Act. The police officers secured criminal history data from the FBI's National Crime Information Center computer and sold it to the detective firm. The fines ranged from $800 to $3,000. This is the only criminal prosecution under the Privacy Act of which I know.

In my book, *Your Right To Privacy*, the final chapter quotes an unnamed private investigator stating, "If there's enough money you can get anything. You have to find the weak link in the chain and go for it. I've never heard of a record I couldn't get if I put my mind to it." Private investigators have bragged that they can

obtain the records of supposedly secret bank accounts from Switzerland, the Cayman Islands and Panama, as well as the contents of bank deposit boxes in the United States.

Weak Privacy Act & The 'Cowboy Atmosphere'

Going back to the "information broker" case, many might ask, "How could this have happened? Aren't there laws against this sort of thing?"

There are many reasons why illegal trafficking in personal data should not come as a surprise. First, the Social Security number increasingly is becoming the personal identifier of choice of both governmental and private organizations. With a name and SSN, the right person sitting in front of the right computer can hop from database to database and extract more and more details about an individual's history, buying habits and movements.

Second, the Privacy Act, which purports to protect our personal data held by the government, is badly in need of an overhaul, as it lacks real remedies for individuals who have suffered invasions of privacy, as well as sanctions for those who violate the law.

It's worth noting that in this case, **the first major attempt to enforce individuals' expectation of privacy in their government-held data, authorities did not even bother to charge those indicted under the Privacy Act. This is because the only criminal sanction available under the Act is a misdemeanor.** In order to gain a felony case, prosecutors had to indict suspects under a Federal bribery statute, and one prohibiting unauthorized access to Federal computers.

On the civil side, individuals whose data were divulged improperly have a very difficult task trying to collect damages under the Privacy Act. Under some court interpretations, an individual can only collect damages if he shows that the improper disclosure was "willful and intentional," and shows that the disclosure caused some actual physical harm or out-of-pocket loss. An exaggerated reading of this standard would conclude that an individual only was entitled to a damages award if the improper disclosure actually caused the individual to fall off his chair and injure his tailbone.

Not only is the Privacy Act antiquated, it has been badly neglected by its primary overseer, the Office of Management and Budget. OMB has statutory authority for coordinating government policy under the Privacy Act, but it primary mission of overseeing budgetary and regulatory matters makes privacy a low priority. Privacy Act coordinators in various agencies for years have complained of OMB's failure to provide guidance under the law, and of lack of resources for training agency personnel.

Thus, the combination of a weak law and ineffective oversight and training created what I call a "Cowboy Atmosphere" in which some Federal employees undoubtedly felt they could divulge supposedly confidential data, profit from it and never get caught because it seemed obvious that "nobody cared."

The solutions to these problems are simple. First, the Privacy Act needs to be amended to strengthen individual rights, including the data subject's civil remedies and criminal sanctions against unethical government employees. Second, an independent Data Protection Board needs to be created to serve as overseer of the Privacy Act, as well as our national privacy policy. Rep. Robert Wise (D-WV) has introduced separate bills to address both of these goals, but the bills have not moved. Action by the Senate would greatly enhance prospects for the two measures. Later I will

discuss how Privacy Commissioners in Canada were able to proscribe unwarranted uses of their identification numbers.

A Brief History On U.S. Information Privacy Policy

A brief look at recent history reveals why the United States, traditionally a pioneer in the field of privacy law and philosophy, is in danger of being designated as having an "inadequate" system for protecting privacy when compared to international standards proposed by the European Community in preparation for "EC '92."

A key starting point is the U.S. Supreme Court's 1976 decision in *U.S. v. Miller* (425 U.S. 435), in which it ruled that under the Constitution, we have no right to information privacy.

Although the Founding Fathers intended that we "be secure in our personal papers," the Burger Court reasoned that when we open a bank account, we voluntarily surrender information about ourselves to the bank. The information then becomes part of the "flow of commerce," and belongs to the bank, not to us. Under the Constitution, the Court ruled, there is no protection for personal information held by third parties. Absent statutory restrictions, the banks therefore were free to give our personal data to anyone they pleased. The message from the Supreme Court was clear: if you want privacy, take your cash home and stick it under the mattress -- or, persuade Congress to act.

The Supreme Court has extended this reasoning to telephone and other third party records. In 1989, the Supreme Court even ruled that we had no constitutional expectation of privacy in our garbage, holding that once put out for collection, our garbage was available to everyone.

Of course none of these decisions were unanimous. Of the garbage ruling, Justice Brennan said the fact that burglars might enter private homes did not negate the right to privacy there. "Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior. I suspect therefore that members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public."

Congress has responded to some of these rulings, enacting statutes that provide differing protections for financial records, telephone records, video store rental data and cable television files. It's not my purpose here to give an overview of U.S. privacy law. Suffice to say that the current state of U.S. privacy law is a patchwork quilt sorely needing attention.

In my 13 years of following the issue, there have been consistent signs confirming that Americans feel strongly about their right to privacy and want stronger legal protections. This has been documented in three separate Lou Harris opinion surveys, the most recent being released in 1990, and a recent survey by *Time Magazine*.

What I have found dramatic in the past few years is the explosion in media attention to the issue, and the subsequent strong public response to that media coverage. Press attention to the uses and abuses of personal data have increased 20-fold, signifying that privacy is emerging as one of the key issues of 1990s. Response to news articles, documentaries and talk shows demonstrates that public is both anxious and angry about the way their personal data are used without notice and consent.

The 1980s' climate for handling personal data virtually dictated that privacy would become a major concern in the 1990s. In the beginning of the 1980s the Reagan Administration completely

turned its back on seven years of bipartisan work by the Ford and Carter Administrations, a federal study commission and Congress to forge a national privacy policy. The Reagan Administration's decision to halt all work on privacy proposals sent a signal to government bureaucrats and certain industries that they could exploit personal data with little or no consideration for individuals' feelings about personal privacy. The 1980's free and easy use of personal data created its own backlash.

The Bush Administration thus far has a mixed record. On the positive side, Dr. Bonnie Guiton, formerly the President's Advisor on Consumer Affairs, made privacy a priority, and brought the privacy and consumer communities together. She raised the visibility of the issue by organizing a national consumer conference on privacy, by testifying in favor of Fair Credit Reporting Act amendments (FCRA), and by creating various task forces and urging industry compliance with voluntary standards. Similarly, the Federal Trade Commission is effectively advocating amendments to strengthen the FCRA.

While the efforts of the U.S. Office of Consumer Affairs have been welcome, its jurisdiction is limited. Meanwhile, the Bush Administration has failed to move on several fronts to improve privacy policy as well as the federal government's own information practices.

Moreover, the Bush Administration steadily has opposed European Community (EC) efforts to strengthen privacy protections worldwide. The Administration appears to be catering to a narrow faction of the business community that prefers unfettered use of personal data and objects to the EC's view that personal data use should be based upon informed consent. In doing so, the Administration finds itself out of step with the vast majority of Americans who favor an informed consent standard. A recent Time Magazine poll showed that 93 percent of American public wanted a law requiring that companies obtain their consent before selling their information to others. (See *Time Magazine*, November 11, 1991, page 36.)

As long as the United States opposes worldwide privacy standards, it will be casting itself in the unenviable role of "the spoiler" in a popular international human rights movement. In fact, the U.S. Government opposed a proposal in the pending GATT accord that simply would allow nations to enact measures to protect personal privacy. Pointing out that U.S. negotiators did not oppose similar provisions on animal or plant life, a European delegate noted the irony, stating, "Certainly, if nations are left free to protect plant life, they should be allowed to protect the privacy of their people." (See *Privacy Times*, December 2, 1991.)

SSN: A Case Study in Erosion of Privacy

The Social Security Card used to state: "This card is not to be used for identification." The promises in the early days that the Social Security number would not become an identification number has turned out to be one of the great lies to the American people, on par with other famous promises like "Your check is in the mail."

Clearly, the history of the Social Security Number (SSN) is a classic case study in the erosion of privacy. The SSN has proved to be the valuable key element that allows computers to talk to eachother, to search through eachother's data files and to draw out individual profiles on people. Accordingly, the creation of one, centralized computer system on all Americans is no longer the only privacy concern. Now the interconnection of small computer networks, made easier by widespread use of the Social Security number, is creating an enormous system capable of data surveillance.

The original use of the SSN, of course, was to number personal accounts for the collection of taxes and benefits in the Social Security program. The first numbers were assigned in 1936. A year later, it was decided that the same identifier should be used to number accounts in state unemployment-insurance systems. In 1943, Executive Order 9397 was issued by President Roosevelt authorizing any federal agency to use the SSN for new data systems requiring permanent account numbers on records pertaining to individuals. This authority was not used for many years, even by the U.S. Civil Service Commission, for whose benefit it was originally intended.

In 1961, the Internal Revenue Service decided to designate the SSN as the taxpayer identification number. Thereafter, new uses followed in rapid succession: for Treasury Bonds, for old-age-assistance benefits accounts, for state and federal civil-service employee records, for Veterans Administration hospital records, Indian Health Service patient records, and as the military-personnel service number.

Congress also encouraged this trend. Under the Tax Reform Act of 1976, it authorized states to use the SSN for motor vehicle registration records and driver's licenses. Currently some three dozen states use the SSN as a driver identification number. As you know, this means that the number often is recorded on checks as an ID number when consumers made purchases. The 1976 law also authorized SSN use for administration of local and state tax laws and of general public assistance programs and for implementation of the Parent Locator System.

Another major step came in 1984, when the Deficit Reduction Act required all depositors to provide to financial institutions their SSNs so IRS computers could match the amount of interest reported by taxpayers with the amounts reported to the IRS by banks.

The law also required recipients of federal benefits to provide social service agencies with their SSNs. The 1986 Tax Reform Act requires parents to show SSNs for children over the age of five who are claimed as dependents.

Despite claims that the SSN was not, or would not become, an personal identification number, it clearly has increasingly become one. Fortunately, though, it does not qualify as a "universal" identifier yet. In hindsight, it should be clear that large institutions with mammoth, computerized data systems will always prefer to seize a common identifying number. To waggle such a tempting tool as an SSN in front of a large government agency or corporation and expect them not to use it is unrealistic -- like trying to roll a lamb chop past a wolf!

That is why strong restrictions on the use of the SSN must be adopted.

Constant Threat To Expand SSN

In recent years, two proposals demonstrated the constant threat of expanding SSN uses. Fortunately, both were defeated.

The first involved an immigration reform proposal to create a "secure" Social Security card that all job applicants would have to show to an employer to prove they could work legally in the United States.

The second involved a proposal to bolster the bank insurance fund. One section would have required that all Americans' bank accounts be recorded under their SSNs in a huge new database to be maintained by the Treasury Department. The system was intended to

ensure that people did not receive more bank insurance fund payments than those to which they were entitled.

Both proposals -- a national work identity card, and a government database on all private bank accounts -- reflected the logical extension of decades of ill-conceived expansion of SSN use. Fortunately, the infeasibility of both proposals, coupled with the enormous surveillance systems they entailed, generated sufficiently strong opposition to defeat them.

My hope is that the defeat of these two proposals represents a watershed, signifying the turning of the tide in the fight to reverse the expansion of SSN uses.

The Private Sector: Out Of Control

Given the proliferation of the use of the SSN by federal and state governments, it's not surprising that the private sector organizations too increasingly have adopted it as their identifier. As mentioned, financial institutions now are required to record their customers' SSNs. But there are plenty of institutions that are not required but do so anyway.

As I was signing up for new natural gas service for my home the Gas Company phone representative asked me several questions and then asked for my SSN. I asked her why the company needed it. She said she wasn't sure. I suggested that we move onto to the next question. She agreed, and was able to provide me with gas service without me giving up my SSN. In the same week, I had nearly identical conversations with the phone representatives of both the cable television and electric company. These companies do not really need the SSN, but everyone is so accustomed to asking for it, they do. And many people are so accustomed to giving it out, they do so without thinking about it.

Is there any harm? That depends on circumstance and the individual's point of view. I receive some two dozen calls a year from people who were irate about always being asked for their SSN.

Not only does the SSN make it easier for large institutions to compare their databases, it allows curious individuals (including private detectives, computer hackers or other strangers you might not want snooping into your private life) to "hop" from database to database and draw out a profile of your buying habits and personal lifestyle. The stranger might go to your Department of Motor Vehicles and get your SSN from your publicly available driver's license. Then using the SSN, he might, albeit illegally, go to a credit bureau and find out what debts you owe, go to an insurance company or the Medical Information Bureau and find out about your health coverage and/or medical condition, check with various publishers to see what magazines you subscribe to and check with a few grocery stores trying out new computerized, "frequent buyer" program to learn what you're buying habits. Access to credit bureaus is illegal, the laws are unenforced. There are few laws barring access to other private sector databases.

Some people do not really care who sees information about them. But as more and more people become aware of how much of their personal information is available, they object to the ease with which it is gathered, shared and stored.

Because current laws are weak, individuals have to be particularly vigilant to block the unnecessary collection of their Social Security number. Take the case of Don Pensa, a New Jersey resident, who recently told me his story. When Mr. Pensa learned that the New Jersey DMV was switching over to the SSN as

the driver's license number, he appealed several times, even writing a letter, until he persuaded the department to grant him an alternative number. It was a difficult process, as the "whole place stood still" upon his suggestion of using a number other than a SSN, Pensa said.

Then, he convinced the Federal Aviation Administration that they did not need his SSN, but could grant him an alternative number for his pilot's license. Pensa reminded FAA officials that they assigned numbers to many foreign pilots who did not even have SSNs.

Next came the fuel oil company. When a phone representative insisted that the company would not open an oil delivery account unless he provided his SSN, Pensa said he would take his business elsewhere. The representative put him on hold for a minute, and then agreed that an account could be opened without an SSN.

Pensa said he was not as lucky with health insurance. In fact, he went many months without health insurance because he could not find an insurer who would provide him coverage if he refused to provide his SSN, he said. Finally, with a little publicity on his side, he convinced an insurer that they did not really need his SSN to provide him with insurance.

Some companies believe that using an SSN is convenient for themselves and their customers, and do not give much consideration to privacy issues. The *Wall Street Journal* reported February 4, 1991 that Fidelity Mutual Funds opened a computerized phone line permitting anyone to learn of a customer's fund holdings and balances by punching in the customer's SSN. A Fidelity marketing manager said the service was very popular and had only been the subject of three complaints. But after the story ran, Fidelity installed additional numbers for accessing the system.

Another New Jersey man recently told me that a company refused to send him a credit card application unless he provided his SSN over the telephone. Most likely, the company wanted to use his SSN to run a credit check on the man, without his knowledge and consent, before sending him the application.

A man in Georgia told me, and I confirmed later, that some banks there would not open a checking account for someone until they had obtained the applicant's SSN and run a credit check.

A Long Island man has refused his insurance company's demand that he sign a waiver granting the company access to all of his Social Security and Railroad Retirement records. The company has cut off the man's disability insurance payments because of his objection to the waiver, which he considered overly broad and an invasion of his privacy.

In the current debate over the Fair Credit Reporting Act, credit bureaus are pushing to make the SSN the official identifier.

Sunshine Is The Best Disinfectant

The media have exposed several questionable practices, causing private companies to alter them. One of the most significant was the public's response to reports about Lotus Marketplace: Households, the set of compact disks with personal data on 120 million Americans. *The Washington Post* reported that some 30,000 consumers told Lotus to remove their names and data before making the product available. This prompted Lotus, and its partner Equifax, the giant credit bureau, to decide the privacy outcry was too much and canceled its plans to offer the product. When consumers asked how they could opt out, they were instructed that they needed to provide their SSNs, as the database feeding the

system was operated by the credit bureau and keyed to SSNs. Similarly, Knight-Ridder exposed a Postal Service plan to keep persons' Christmas card mailing lists in a USPS computer.

In 1989, the *New York Times* exposed a secret program under which the Social Security Administration matched its database against sample databases submitted separately by Citibank and TRW, the credit bureau. After the story, and issuance of an Congressional Research Service Opinion that the program violated the federal Privacy Act, SSA ended the practice. Documents obtained by *PRIVACY TIMES* showed that both the match with Citibank and with TRW uncovered more than a 30 percent error rate among somebody's list of SSNs, presumably TRW's and Citibank's. This little-noticed fact raises questions about the accuracy of some private sector databases.

It should not be a surprise that there were major inaccuracies in the SSNs maintained by private sector organizations. SSNs regularly are stolen, lost, shared, intentionally altered or accidently transposed. In sum, they are vulnerable to changes which render them inaccurate, and thus, an ineffective personal identifier. Accordingly, it is likely that there will always be pressure on the government to run SSN verification schemes, similar to what SSA did for Citicorp and TRW. But that is an ill-conceived policy that will not achieve its objective and at the same time will set disastrous precedents for our national privacy, and will greatly expands the lie to the American people the SSN would never be used for identification purposes.

I hope the subcommittee can secure a public commitment from the SSA Commissioner never to engage in SSN verification schemes.

The Privacy Act & SSN Use

The Privacy Act requires government agencies demanding SSNs to:

(1) cite its formal legal authority for using the number,
(2) reveal whether disclosure is mandatory or voluntary and
(3) explain how the number will be used.

I hope the above account makes it clear that the Privacy Act's "restrictions" on use of the SSN are of questionable value and that much stronger measures are needed if we are to restore to individuals the privacy and integrity they deserve.

Some General Solutions

(1) Congress should pass a law placing a moratorium on use of the SSN by all institutions not already authorized by law to use it.

(2) Congress should require that any future proposals to expand the SSN be referred to this subcommittee and its counterpart in the House. Only that way will the proposal receive the attention it deserves and the benefit of the subcommittee's expertise.

(3) Congress should amend the Privacy Act to provide tougher criminal sanctions, stronger civil remedies and more controls on agency sharing of personal data.

(4) Create an independent national office to be in charge of U.S. privacy policy, to make legislative recommendations to Congress, to oversee the Privacy Act, to serve as a resource to the public and the media when they need information about or help with a privacy issue.

I can't emphasize enough the importance of the United States having an independent office in charge of our national privacy policy. In other countries such offices have played important roles.

Two notable examples concerned limits on the use of identification numbers. A few years ago in Ottawa, then Privacy Commissioner John Grace recommended that the Canadian Government conduct a complete review of its agencies's use of their Social Insurance Number (SIN), and restrict its use when found to be unnecessary and inappropriate. Grace had no authority to order this change. But the Canadian Government carried out Grace's recommendation. For the first time it identified the ways in which the SIN was being used and actually halted its use in a few cases.

Last year, the Ontario Provincial Government adopted a new health identification number to be used by provincial citizens under the health plan. The Ontario Office of the Information and Privacy Commissioner studied the issue and recommended strict curbs on use of the number. The Government instituted the commissioner's recommendation as provincial policy.

WHAT THE SUBCOMMITTEE CAN DO NOW

I hope you will hold additional hearings on the Social Security number and privacy issues. You will find that the attention you focus on the issue provides important public education and raises public awareness -- an important development in itself.

While we have some anecdotal evidence, we really do not have a comprehensive survey of how the SSN is used in the public and private sectors.

It would be important to know if federal agencies are complying with Section 7 of the Privacy Act, which concerns their obligation to inform individuals if disclosure of their SSNs is mandatory or voluntary. The section was intended by Congress to prohibit coercing individuals into divulging their SSN when it was not necessary. But it's not clear what impact this Section is having on agency practices.

Similarly, we do not know the extent to which the SSN is used in the private sector for non-employment purposes. We also do not know to what extent advances in technology permit companies that use the SSN as a customer identification number to manipulate personal information and create consumer profiles.

Accordingly, the subcommittee should:

(1) Order a two-track survey by the appropriate research office (GAO, OTA, CRS, CBO, etc) which:

(a) Explores the extent to which federal, state and local agencies are complying with Privacy Act Section 7; and

(b) Documents the extent to which private sector organizations are using the SSN as an identifier when they are not required to by law.

(2) Request that the Office of Technology Assessment study the effectiveness or ineffectiveness of the SSN as an accurate identifier, and explore the feasibility of alternative identifiers that would be more effective and privacy-enhancing than the SSN.

(3) Secure a public commitment from the SSA Commissioner that the SSA will no longer take part SSN verification schemes.

Mr. Chairman, advancing the cause of privacy is an interest the entire public shares. An important part of advancing privacy is leadership by individual members of Congress. Sen. Sam Ervin's legendary efforts on behalf of privacy and justice are well known, and have appropriately earned him an important place in U.S. history.

In recent years, Sen. Patrick Leahy (D-VT) has been the Senate's main champion of privacy. But the privacy issue is growing exponentially, cutting across all sectors of our life -- government, credit, medical, insurance, employment and consumer. That is why the privacy movement needs -- and welcomes -- additional leaders on Capitol Hill.

As I've indicated, there are legislative solutions to many of the privacy problems facing us. But they require Congress to move on several fronts and to engage in the challenging process of enacting laws which strike the proper balance. I hope that these hearings will lead to new proposals to control the SSN, and that other Congressional panels will follow your lead in areas over which they have jurisdiction.

In closing, I would like to quote a passage from Supreme Court Justice William O. Douglas, another champion of privacy.

In opposing Bank Secrecy Act requirements that all customer checks be recorded and available for government inspection, Supreme Court Justice William O. Douglas in 1974 prophesied that the fight against money laundering had started our nation down a slippery slope in which privacy increasingly would be sacrificed:

> It would be highly useful to governmental espionage to have like reports from all our bookstores, all our hardware and retail stores, all our drug stores. These records also might be 'useful' in criminal investigations. . . .
>
> A mandatory recording of all telephone conversations would better than the recording of checks under the Bank Secrecy Act, if Big Brother is to have his way. . . .
>
> In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads and so on ad infinitum. These are all tied to one's Social Security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat -- by pushing one button -- to get in an instant the names of 190 million Americans who are subversives or potential and likely candidates. (*California Bankers Association v. Shultz*, 416 U.S. 735, 1974.)

Mr. Chairman, again I would like to thank the Committee for the opportunity to testify on this very important matter. I would be happy to answer any questions.

PREPARED STATEMENT OF LARRY D. MOREY

GOOD MORNING, I AM LARRY MOREY, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES. THANK YOU FOR THE OPPORTUNITY TO TESTIFY ON THE SOCIAL SECURITY ADMINISTRATION AND ITS PROGRAMS. I WOULD LIKE TO FOCUS MY REMARKS ON OUR RESPONSIBILITY FOR SAFEGUARDING CONFIDENTIAL INFORMATION ON AMERICAN CITIZENS CONTAINED IN THE SOCIAL SECURITY ADMINISTRATION'S COMPUTERIZED RECORDS SYSTEMS, AS WELL AS SOCIAL SECURITY NUMBER FRAUD. I WILL ALSO PROPOSE OPTIONS FOR IMPROVING EFFICIENCY AND REDUCING FRAUD IN THIS AREA.

OVERVIEW OF THE OIG

AS YOU KNOW, THE OFFICE OF INSPECTOR GENERAL (OIG) HAS A STATUTORY RESPONSIBILITY TO PROTECT THE INTEGRITY OF DEPARTMENTAL PROGRAMS AS WELL AS THE HEALTH AND WELFARE OF BENEFICIARIES SERVED BY THOSE PROGRAMS. THROUGH OUR COMPREHENSIVE AUDITS, PROGRAM INSPECTIONS, AND INVESTIGATIONS, WE PROMOTE EFFICIENCY AND EFFECTIVENESS IN THE DEPARTMENT'S PROGRAMS AND DETECT FRAUD, WASTE, AND ABUSE.

THE OIG ROUTINELY EXAMINES THE SOCIAL SECURITY ADMINISTRATION AND ITS PROGRAMS. OUR SOCIAL SECURITY INVESTIGATIONS FOCUS ON THREE BASIC AREAS, WHICH OFTEN OVERLAP -- FRAUD BY EMPLOYEES OF THE SOCIAL SECURITY ADMINISTRATION, BENEFITS FRAUD INVOLVING EACH OF THE SOCIAL SECURITY PROGRAMS, AND SOCIAL SECURITY NUMBER (SSN) FRAUD. IN ADDITION, AS PART OF ITS STATUTORY MANDATE, THE OIG ANALYZES THE INTERNAL CONTROLS AND SECURITY MEASURES THAT HAVE BEEN BUILT INTO THE SSA SYSTEMS TO ENSURE THAT PROGRAM VULNERABILITIES DO NOT EXIST. OUR REPORTS HAVE MADE RECOMMENDATIONS FOR CONTROLLING ACCESS AND DISCLOSURE OF DATA.

OVERVIEW OF THE SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION (SSA) IS RESPONSIBLE FOR PROGRAMS INCLUDING THE RETIREMENT, SURVIVORS, AND DISABILITY

INSURANCE PROGRAMS FINANCED BY THE SOCIAL SECURITY TRUST FUNDS. SSA ALSO ADMINISTERS THE SUPPLEMENTAL SECURITY INCOME (SSI) AND BLACK LUNG PROGRAMS, WHICH ARE FUNDED FROM GENERAL REVENUES. TOTAL EXPENDITURES FOR THESE PROGRAMS IS EXPECTED TO REACH $300 BILLION IN FISCAL YEAR 1993.

THE SSA ALSO PROVIDES SERVICE TO THE PUBLIC THROUGH ISSUANCE OF NEW AND REPLACEMENT SOCIAL SECURITY CARDS AND MAINTENANCE OF EARNINGS RECORDS FOR ALL WORKERS. THE SSA ISSUED 19.7 MILLION NEW AND REPLACEMENT SOCIAL SECURITY CARDS IN FY 1990, COMPARED TO 17.6 MILLION IN FY 1989.

SOCIAL SECURITY NUMBERS (SSNs) ARE USED PRIMARILY BY SSA TO MAINTAIN THE EARNINGS RECORDS OF 140 MILLION WORKERS. THE RECORDS ARE USED TO DETERMINE IF AN INDIVIDUAL QUALIFIES FOR BENEFITS AND TO INSURE THE CORRECT AMOUNT OF BENEFITS ARE PAID. SSA HAS IDENTIFIED THE ASSIGNMENT OF SSNS AS A STRATEGIC AREA WITH EMPHASIS ON ISSUING SSNs PROMPTLY WHILE MAINTAINING THE INTEGRITY OF THE NUMBER.

THE SSN IS WIDELY USED BY BOTH THE PUBLIC AND PRIVATE SECTORS. IN AUGUST 1988, WE ISSUED A REPORT ENTITLED "EXTENT OF USE OF SOCIAL SECURITY NUMBERS". WE FOUND THAT AN OVERWHELMING MAJORITY OF PUBLIC AND PRIVATE SECTOR AGENCIES USE SSNS AS A NORMAL PART OF THEIR OPERATIONS. OF THE RESPONDING AGENCIES, 81 PERCENT USED SSNS ROUTINELY AS AN IDENTIFIER.

SYSTEMS MODERNIZATION

TO THEIR CREDIT, SSA HAS MADE MAJOR ADVANCEMENTS IN SYSTEMS MODERNIZATION IN THE LAST TEN YEARS, ENABLING DRAMATIC IMPROVEMENTS IN THE TIMELINESS AND QUALITY OF ITS SERVICE TO THE PUBLIC. SSA HAS INVESTED OVER $600 MILLION IN THIS EFFORT. SSA EMPLOYEES CAN NOW PROCESS BENEFIT CLAIMS AND RETRIEVE BENEFIT AND EARNINGS INFORMATION ON NEARLY 140 MILLION WORKERS IN MINUTES OR

SECONDS RATHER THAN DAYS. SYSTEMS MODERNIZATION HAS ALLOWED SSA TO IMPROVE SERVICE DELIVERY IN A NUMBER OF AREAS. FOR EXAMPLE:

- REDUCE FROM 6 WEEKS TO 10 DAYS THE TIME IT TAKES TO ISSUE SOCIAL SECURITY CARDS;
- POST ANNUAL WAGE REPORTS IN 6 MONTHS INSTEAD OF 4 YEARS;
- LOWER THE TIME IT TAKES TO CALCULATE ANNUAL BENEFIT INCREASES FROM 4 YEARS TO 6 MONTHS;
- PAY EMERGENCY PAYMENTS IN 5 DAYS INSTEAD OF 15 DAYS.

AS PART OF THIS SYSTEM MODERNIZATION, SSA CONVERTED MANY OF ITS FILES TO ON-LINE DATA BASES. AS A RESULT OF THESE EFFORTS, AUTHORIZED SSA EMPLOYEES CAN NOW PROCESS SSN APPLICATIONS AND BENEFIT CLAIMS AND RETRIEVE DETAILED BENEFIT AND EARNINGS INFORMATION ALMOST IMMEDIATELY. WHILE SSA HAS TAKEN STEPS TO SAFEGUARD THESE RECORDS, THIS INCREASED ACCESS HAS BROUGHT WITH IT NEW THREATS TO THE CONFIDENTIALITY OF RECORDS.

INVESTIGATING INFORMATION DISCLOSURE FRAUD

YOUR REQUEST ASKED US TO SPECIFICALLY LOOK AT ACCESS TO SOCIAL SECURITY INFORMATION AND ITS DISCLOSURE. THE COMPUTER SECURITY ACT OF 1987 REQUIRES THAT FEDERAL AGENCIES ESTABLISH A PLAN FOR THE SECURITY AND PRIVACY OF THEIR COMPUTER SYSTEMS TO PROTECT AGAINST LOSS, MISUSE, OR UNAUTHORIZED ACCESS TO OR MODIFICATION OF THE INFORMATION CONTAINED IN THESE SYSTEMS. IN ADDITION, UNDER THE SAFEGUARDS OFFERED BY THE PRIVACY ACT OF 1974 AND THE SOCIAL SECURITY ACT, RELEASE OF THIS INFORMATION IS GENERALLY RESTRICTED TO OFFICIAL USE.

HOWEVER, BECAUSE OF THE EXTREMELY HIGH MARKETABILITY OF SOCIAL SECURITY NUMBERS AND RECORDS, WE CONTINUE TO INVESTIGATE A LARGE NUMBER OF CASES INVOLVING THE ILLEGAL SALE, USE -- AND IN SOME CASES, ALTERATION -- OF SOCIAL SECURITY NUMBERS AND CARDS.

SOCIAL SECURITY NUMBER FRAUD

THE SSN IS A CRITICAL ELEMENT OF IDENTIFICATION USED IN NEARLY EVERY SECTOR OF AMERICAN SOCIETY. AS SUCH, IT HAS BEEN TARGETED FOR ABUSE IN A WIDE VARIETY OF CRIMINAL ACTIVITIES. THE SSN CAN BE USED TO OBTAIN SOCIAL SECURITY OR OTHER GOVERNMENT BENEFITS, DRIVER'S LICENSES, CREDIT CARDS, AND PASSPORTS. WE OFTEN SEE PERSONS WHO COMMIT A WIDE RANGE OF CREDIT FRAUD AND OTHER CRIMES, USING FALSE SSNs TO CONCEAL THEIR TRUE IDENTITY. THE FEDERAL IDENTIFICATION FRAUD REPORT ISSUED BY THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS IN MAY 1983, ESTIMATED THE ECONOMIC IMPACT OF FALSE IDENTIFICATION FRAUD ON GOVERNMENT AND COMMERCE TO BE $24 BILLION ANNUALLY.

SINCE 1983, THE CRIMES BASED ON FALSE IDENTIFICATION DOCUMENTS HAVE INCREASED SIGNIFICANTLY, AS HAVE OUR CONVICTIONS IN THE SOCIAL SECURITY NUMBER AREA. MANY LAW ENFORCEMENT AND REGULATORY AGENCIES RELY ON THE OIG FOR ASSISTANCE IN IDENTIFYING, LOCATING, INVESTIGATING, AND PROSECUTING INDIVIDUALS WHO HAVE IMPROPERLY USED SSNs IN A BROAD RANGE OF ILLEGAL ACTIVITIES. IN A LARGE NUMBER OF OUR CASES, THE SSN VIOLATION MAY BE THE ONLY BASIS FOR A CONVICTION, EVEN WHEN OTHER SERIOUS CRIMES HAVE BEEN COMMITTED.

OF THE 1,066 CRIMINAL CONVICTIONS THE OIG OBTAINED IN FISCAL YEAR 1991 RELATING TO FRAUD IN SOCIAL SECURITY PROGRAMS, 590 INVOLVED UNLAWFUL USE OF SSNs. LET ME PROVIDE YOU WITH A RECENT EXAMPLE OF AN SSN FRAUD CASE.

- A CANADIAN MAN WAS SENTENCED TO 2 1/2 YEARS IN JAIL FOR USING A FRAUDULENT SSN IN ATTEMPTING TO NEGOTIATE A STOLEN CERTIFICATE FOR 192,800 PHARMACEUTICAL COMPANY SHARES. THE CERTIFICATE, WORTH MORE THAN $7 MILLION AT THE TIME, WAS ONE OF SEVERAL STOLEN FROM A COURIER IN LONDON. THE MAN DEPOSITED THE CERTIFICATE WITH A STOCKBROKER IN VIRGINIA, USING AN SSN ISSUED LAST APRIL TO AN INFANT IN SOUTH CAROLINA. AS PART OF HIS PLEA, HE AGREED TO COOPERATE IN TRACING THE MOVEMENT OF THE OTHER CERTIFICATES. TOTAL VALUE OF THE CERTIFICATES IS ESTIMATED AT $70 MILLION.

SSA HAS MADE SIGNIFICANT IMPROVEMENTS TO THE SSN APPLICATION PROCESS. ALL INDIVIDUALS OVER AGE 18 ARE REQUIRED TO APPLY FOR AN SSN IN PERSON AND PRESENT EVIDENCE OF AGE, IDENTITY AND CITIZENSHIP OR ALIEN STATUS. RANDOM SAMPLES OF SSN APPLICATIONS ARE SYSTEMATICALLY REVIEWED BY MANAGEMENT. NEVERTHELESS, THE SSN APPLICATION PROCESS IS CONSISTENTLY VICTIMIZED BY INDIVIDUALS INTENT ON OBTAINING AN SSN UNDER FALSE PRETENSES.

SSA SHOULD TAKE MORE PROACTIVE STEPS TO TARGET HIGH RISK APPLICATIONS -- THOSE FROM U.S. BORN ADULTS AND FOREIGN BORN APPLICANTS -- FOR MORE RIGOROUS REVIEW. FOR APPLICATIONS ALLEGING NO PRIOR SSN, SSA SHOULD DEVELOP PROCEDURES TO VERIFY THE DOCUMENTS PRESENTED, AS WELL AS THE APPLICANT'S REASONS FOR NOT HAVING AN SSN.

TO ASSIST SSA IN THIS EFFORT, WE ARE PLANNING A STUDY ON SOCIAL SECURITY CLAIMS UNDER FALSE OR ASSUMED IDENTITIES TO DETERMINE IF A PROFILE DEVELOPED FROM INVESTIGATIONS OF MULTIPLE FALSE IDENTITY CASES WOULD FACILITATE THE SYSTEMATIC DETECTION AND PREVENTION OF FALSE IDENTITY SCHEMES. DATA GATHERED DURING OUR INVESTIGATIONS WILL BE ANALYZED TO DEVELOP A PROFILE OF HIGH RISK CASES. SSA WILL BE ABLE TO USE THE PROFILE TO ENHANCE ITS PROCEDURES FOR EVALUATING DOCUMENTS SUBMITTED AS EVIDENCE AND OPERATING PROCEDURES FOR THE HANDLING OF QUESTIONABLE DOCUMENTS.

ILLEGAL DISCLOSURE OF CONFIDENTIAL INFORMATION

YOU HAVE ALSO REQUESTED THAT WE DISCUSS THE PROBLEM OF DISCLOSURE THROUGH THE USE OF SSA EMPLOYEES. I WOULD NOTE THAT THE MAJORITY OF SSA'S 63,000 EMPLOYEES ARE HONEST, DEDICATED, AND WELL-TRAINED. AS PART OF OUR STATUTORY MANDATE, HOWEVER, WE DO CONDUCT INVESTIGATIONS OF SUSPECTED MISCONDUCT BY SSA EMPLOYEES. SINCE 1983, WE HAVE INVESTIGATED ABOUT 900 ALLEGATIONS INVOLVING MISCONDUCT. APPROXIMATELY 200 OF THESE ALLEGATIONS INVOLVED THE DISCLOSURE OF CONFIDENTIAL INFORMATION OR OTHER MISUSE OF SSA

COMPUTER SYSTEMS. OF THESE, AN ESTIMATED 70 CASES RESULTED IN CRIMINAL CONVICTIONS.

THE NATURE OF THE INFORMATION HOUSED IN SSA RECORDS -- COMBINED WITH THE TECHNOLOGICAL ADVANCES THAT MAKE THIS INFORMATION IMMEDIATELY ACCESSIBLE -- MAKE THESE RECORDS AN ATTRACTIVE TARGET FOR PEOPLE OR ORGANIZATIONS ATTEMPTING TO LOCATE INDIVIDUALS OR AUTHENTICATE INFORMATION SUPPLIED TO THEM. PROTECTING THE CONFIDENTIALITY OF THIS INFORMATION IS A MAJOR CONCERN, BOTH TO THE OIG AND THE SSA. WE ARE IN AGREEMENT THAT ANY BREACH IN THE SECURITY ARRANGEMENTS THAT HAVE BEEN ESTABLISHED TO PROTECT PERSONAL INFORMATION IS A VERY SERIOUS MATTER.

RECENTLY, WE HAVE SEEN AN EXPANSION IN THE NUMBER OF "INFORMATION BROKERS" WHO ATTEMPT TO OBTAIN, BUY, AND SELL SSA INFORMATION TO PRIVATE COMPANIES, FOR THEIR USE IN LOCATING PEOPLE OR MAKING DECISIONS ON HIRING, FIRING, SUING OR LENDING. AS THE DEMAND FOR THIS INFORMATION GROWS, THESE BROKERS ARE TURNING TO INCREASINGLY ILLEGAL METHODS. FOR EXAMPLE, WE HAVE A CASE INVOLVING NATIONWIDE ELECTRONIC TRACKING (NET), A FLORIDA BASED FIRM WHICH PROMISES "INSTANT ACCESS" TO "CONFIDENTIAL DATA...24 HOURS A DAY, 7 DAYS A WEEK." THIS CASE IS THE LARGEST EVER PROSECUTED INVOLVING THE THEFT OF FEDERAL COMPUTER DATA:

- 23 INDIVIDUALS -- INCLUDING PRIVATE INVESTIGATORS, DEPARTMENT EMPLOYEES, AND LAW ENFORCEMENT OFFICERS -- WERE RECENTLY INDICTED BY FEDERAL GRAND JURIES IN FLORIDA AND NEW JERSEY FOR BUYING AND SELLING CONFIDENTIAL INFORMATION HELD IN GOVERNMENT COMPUTERS. THE INFORMATION RELEASED INCLUDED SSA EARNINGS INFORMATION; SSNs; FULL NAMES; DATES OF BIRTH; NAMES OF PARENTS; NAMES OF ALL CURRENT AND PAST EMPLOYERS; SALARY INFORMATION; AND OTHER NON-PUBLIC INFORMATION.

  THIS ON-GOING INVESTIGATION REVEALED THAT THE GOVERNMENT EMPLOYEES WERE ALLEGEDLY BRIBED OR DUPED FOR ACCESS TO THE INFORMATION, WHICH WAS THEN SOLD. OIG INVESTIGATORS SET UP "DUMMY" TRANSACTIONS THROUGH THE N.E.T. FIRM, PLANTING NAMES OF PEOPLE TO BE CHECKED AND THEN ALERTING SSA OFFICIALS SO THEY COULD BE ON GUARD WHEN EMPLOYEES PUNCHED THOSE NAMES INTO THE COMPUTERS.

WE HAVE IDENTIFIED THREE QUESTIONABLE METHODS USED BY THESE BROKERS TO OBTAIN SSA INFORMATION. FIRST, THE BROKER WILL HAVE ONE OR MORE SSA EMPLOYEES "UNDER CONTRACT". THESE EMPLOYEES SELL EARNINGS HISTORIES TO THE BROKERS FOR ABOUT $25 APIECE, WHICH IN TURN MARK UP THE PRICE TO $300 OR MORE. THE BROKERS TEND TO HAVE A SET FEE SCHEDULE, DEPENDING ON THE TYPE OF INFORMATION REQUESTED AND HOW QUICKLY IT IS NEEDED. AMONG THE MOST REQUESTED TYPES OF SSA INFORMATION ARE THE DETAILED EARNINGS QUERY (DEQY), NUMIDENT, AND THE MASTER BENEFICIARY RECORD (MBR). THE FOLLOWING IS A DESCRIPTION OF EACH TYPE:

- THE **DEQY** PROVIDES EMPLOYER NAMES AND ADDRESSES AND THE AMOUNTS EARNED BY YEAR. IN ADDITION, THE QUERY PROVIDES THE LAST NAME AND FIRST INITIAL OF THE NUMBER HOLDER, OTHER NAMES USED, AND THE MONTH AND YEAR OF BIRTH. IT IS VALUABLE, NOT ONLY FOR THIS INFORMATION, BUT ALSO BECAUSE IT PROVIDES A LEAD TO THE NUMBER HOLDER'S WHEREABOUTS.

- **NUMIDENT** RECORDS CONTAIN THE INFORMATION FURNISHED ON SSN APPLICATIONS. IT PROVIDES THE NAME(S), DATE OF BIRTH, PLACE OF BIRTH, MOTHER'S MAIDEN NAME, AND FATHER'S NAME AS SHOWN ON ORIGINAL APPLICATION, AS WELL AS ANY SUBSEQUENT APPLICATIONS FOR REPLACEMENT CARDS. THE QUERY ALSO SHOWS CODES IDENTIFYING THE ALIEN/CITIZENSHIP STATUS OF THE APPLICANT, THE SSA OFFICE WHERE PROCESSED, AND THE DATE PROCESSED. THE NUMIDENT WILL ALSO INDICATE IF SSA HAS A REPORT OF DEATH FOR THE NUMBER HOLDER. THIS INFORMATION CAN HELP INDIVIDUALS ESTABLISH FALSE IDENTITIES.

- THE **MBR** PROVIDES COMPREHENSIVE INFORMATION PERTAINING TO CERTAIN BENEFICIARIES. AN MBR IS VALUABLE TO INFORMATION BROKERS BECAUSE IT SHOWS THE BENEFICIARY'S CURRENT ADDRESS, DIRECT DEPOSIT INFORMATION -- BANK ROUTING NUMBER AND ACCOUNT NUMBER -- THE BENEFICIARY'S TELEPHONE NUMBER, BENEFIT AMOUNTS, DATE OF BIRTH, AND FAMILY COMPOSITION.

SECOND, THE BROKER CAN GO THROUGH AN ENTITY WHICH HAS LEGITIMATELY CONTRACTED WITH SSA TO OBTAIN EARNINGS RECORD INFORMATION. THESE ENTITIES INCLUDE PRIVATE INVESTIGATORS, INSURANCE COMPANIES, LAW ENFORCEMENT PERSONNEL, ATTORNEYS, CREDIT UNIONS, AND EMPLOYMENT AGENCIES. THE CONTRACT HOLDER FURNISHES A FORGED SSN RELEASE FORM TO THE SSA OFFICE OF CENTRAL RECORDS OPERATION, WHICH THEN SUPPLIES THE INFORMATION WITHIN 6 WEEKS.

A THIRD SCHEME USED, ESPECIALLY BY PRIVATE INVESTIGATORS, IS CALLED "PRETEXTING." THE INVESTIGATOR CALLS AN SSA OFFICE,

USUALLY A TELESERVICE CENTER (TSC), CLAIMING TO BE AN SSA EMPLOYEE FROM ANOTHER OFFICE WHERE THE COMPUTERS ARE DOWN. THE TSC EMPLOYEE IS REQUESTED TO OBTAIN THE INFORMATION AND READ IT OVER THE PHONE. THE INVESTIGATOR SIMPLY WRITES DOWN THE DESIRED INFORMATION AND PASSES IT ON TO HIS CLIENT.

THE SSA HAS TAKEN SIGNIFICANT STEPS TO PROTECT ITS DATA BASES FROM MISUSE AND UNAUTHORIZED ACCESS, INCLUDING MONITORING OF ITS DATA. FOR EXAMPLE, SSA OFFICIALS ARE KEEPING CLOSER TABS ON EMPLOYEES WHOSE PERSONAL COMPUTER CODES ENABLE THEM TO ACCESS INFORMATION. IN ADDITION, THE SSA RECENTLY ISSUED PROCEDURES REQUIRING REGIONAL SECURITY STAFF TO MORE CLOSELY CONTROL INFORMATION RELEASED TO LOCAL MANAGERS FOR REVIEW. DESPITE THESE PRECAUTIONS, WE FIND PROBLEMS WITH SSA MONITORING OF EMPLOYEE ACCESS TO CONFIDENTIAL DATA AND THE ILLEGAL DISCLOSURE OF THIS INFORMATION BY EMPLOYEES. BASED ON INVESTIGATIVE AND AUDIT RESULTS, OUR PRELIMINARY FINDINGS ARE DISCUSSED BELOW:

- SSA DOES NOT SYSTEMATICALLY MONITOR USE OF NUMIDENT QUERIES OF DEQYS;
- INFORMATION DISCLOSED THROUGH CONTRACT AUTHORIZATIONS AND ROUTINE DISCLOSURE PROCEDURES ADMINISTERED BY SSA'S OFFICE OF CENTRAL RECORDS OPERATIONS WERE NOT ADEQUATELY CONTROLLED; AND,
- SSA FIELD OFFICES HAVE DISCLOSED DATA TO CALLERS WHO FALSELY IDENTIFY THEMSELVES AS SSA EMPLOYEES OR AS SSN HOLDERS.

WE HAVE MADE SEVERAL RECOMMENDATIONS TO SSA, WHICH I WILL DISCUSS LATER IN MY TESTIMONY. SSA OFFICIALS HAVE TOLD US THAT THESE SUGGESTIONS WILL HELP THEM ADJUST SECURITY PROCESSES AND MAKE THEM MORE EFFECTIVE.

WE ALSO RECOGNIZE THAT THE OIG'S OWN SECURITY PROCESSES CAN BE STRONGER. CONSEQUENTLY, WE ARE REEVALUATING OUR COMPUTER SECURITY, INVESTIGATING HOW TO INCREASE LEVELS OF SECURITY AND ACCESS. AMONG THE STEPS TAKEN IS A REDUCTION IN THE NUMBER OF OIG EMPLOYEES WHO CAN MAINTAIN PERSONAL IDENTIFICATION NUMBERS (PINs). WE HAVE ALSO IMPLEMENTED PROCEDURES IN ORDER TO BETTER

SAFEGUARD DATA OBTAINED FROM THE SSA SYSTEMS AND PROVIDE ADDITIONAL DOCUMENTATION FOR EACH USE OF THE SYSTEM. THIS WILL NOT ONLY BETTER PROTECT THE RECORDS BUT WILL ALSO PROVIDE A MECHANISM TO ACCOUNT FOR EMPLOYEE USE OF SSA DATA.

PROGRAM VULNERABILITIES

IN ADDITION TO CONDUCTING INVESTIGATIONS, THE OIG HAS ALSO UNDERTAKEN A NUMBER OF REVIEWS CONCERNING SOCIAL SECURITY NUMBERS, AS WELL AS INTERNAL CONTROLS AND SECURITY MEASURES IN SSA'S COMPUTER SYSTEMS. OUR REVIEWS HAVE FOCUSED ON THE VULNERABILITY OF THE PROCESS TO EMPLOYEE ABUSE OR APPLICANTS INTENT ON USING SSNs AND RECORDS ILLEGALLY. I WOULD LIKE TO SUBMIT THESE REPORTS FOR THE RECORD.

THE OIG HAS ALSO ISSUED TWO REPORTS THAT HAVE A CLOSE CORRELATION WITH THE SOCIAL SECURITY NUMBER PROCESS. THE REPORTS, "BIRTH CERTIFICATE FRAUD" AND "BIRTH CERTIFICATE FRAUD UPDATE", WERE RELEASED IN MARCH 1988 AND NOVEMBER 1991, RESPECTIVELY. THE PURPOSE WAS TO SUMMARIZE EFFORTS TO CONTROL BIRTH CERTIFICATE FRAUD. WE FOUND THAT SSA IS TAKING STEPS TO REDUCE BIRTH CERTIFICATE FRAUD IN ITS PROGRAMS. HOWEVER, EFFORTS AMONG FEDERAL AND STATE AGENCIES TO PREVENT BIRTH CERTIFICATE FRAUD LACK COORDINATION. WE CONCLUDED THAT A TIGHTENING OF STATE PROCEDURES CONCERNING THE ISSUANCE OF BIRTH CERTIFICATES IS NEEDED TO CONTROL BIRTH CERTIFICATE FRAUD. WE RECOMMENDED THAT SECURITY OF EXISTING STATE DOCUMENTS, SPECIFICALLY BIRTH CERTIFICATES AND DRIVER'S LICENSES, BE STRENGTHENED AND THAT STRICTER EVIDENTIARY REQUIREMENTS BE USED FOR ISSUING SSNs.

WE HAVE ALSO BEEN EXAMINING THE USE OF THE SOCIAL SECURITY NUMBER IN THE PRIVATE SECTOR. IN FEBRUARY 1990, WE ISSUED A REPORT ENTITLED "EXTENT OF SOCIAL SECURITY NUMBER DISCREPANCIES". WE EXAMINED THE RECORDS OF 36 PUBLIC AND PRIVATE ENTITIES. WE FOUND

THAT 50 PERCENT OF THOSE ORGANIZATIONS HAD SSN DISCREPANCIES OF 10 PERCENT OR MORE.

OF THESE, THE FINANCIAL INSTITUTIONS HAD DISCREPANCY RATES OF 17 PERCENT. THESE INSTITUTIONS ARE REQUIRED TO OBTAIN THE SSN OF THEIR CUSTOMERS IN ORDER TO REPORT INTEREST INCOME TO THE INTERNAL REVENUE SERVICE. THIS DATA IS USED BY SSA TO MONITOR THE INCOME AND RESOURCES OF INDIVIDUALS RECEIVING SUPPLEMENTAL SECURITY INCOME PAYMENTS. CURRENTLY, HOWEVER, SSA DOES NOT PERMIT FINANCIAL INSTITUTIONS TO VERIFY THE ACCURACY OF SSNs IN THEIR RECORDS.

MATERIAL WEAKNESSES

I WOULD NOW LIKE TO DISCUSS THE ROLE WE PLAY IN THE DEPARTMENT'S IMPLEMENTATION OF THE FEDERAL MANAGERS FINANCIAL INTEGRITY ACT (FMFIA) OF 1982. THE CONGRESS ENACTED THE FMFIA IN RESPONSE TO CONTINUING DISCLOSURES OF WASTE, LOSS, UNAUTHORIZED USE, AND MISAPPROPRIATION OF FUNDS OR ASSETS ACROSS A WIDE SPECTRUM OF GOVERNMENT OPERATIONS. THE GOAL OF THIS LEGISLATION WAS TO HELP REDUCE FRAUD, WASTE, AND ABUSE, AS WELL AS TO ENHANCE MANAGEMENT OF FEDERAL GOVERNMENT OPERATIONS THROUGH IMPROVED INTERNAL CONTROLS AND ACCOUNTING SYSTEMS. THE FMFIA PLACED THE PRIMARY RESPONSIBILITY FOR ADEQUATE CONTROL AND ACCOUNTING SYSTEMS WITH AGENCY MANAGEMENT. THE ACT REQUIRES AGENCY HEADS TO REPORT ANNUALLY TO THE PRESIDENT AND TO THE CONGRESS ON THE STATUS OF THE DEPARTMENT'S INTERNAL CONTROLS AND ACCOUNTING SYSTEMS AND PROVIDES FOR THE DISCLOSURE OF MATERIAL WEAKNESSES.

THE OIG HAS BEEN ACTIVELY INVOLVED IN THE FMFIA PROCESS SINCE ITS INCEPTION. WE IDENTIFY DEFICIENCIES THAT MAY CONSTITUTE A "MATERIAL WEAKNESS" UNDER THE FMFIA, MAKE SPECIFIC RECOMMENDATIONS TO CORRECT PROBLEMS, MONITOR CORRECTIVE ACTION TAKEN, ADVISE TOP MANAGEMENT ON INTERNAL CONTROL ISSUES, REVIEW THE FMFIA ANNUAL REPORT, AND AUDIT FINANCIAL STATEMENTS.

SINCE THE INCEPTION OF FMFIA, SSA HAS REPORTED 26 INTERNAL CONTROL AND ACCOUNTING PROBLEMS. OF THESE 26 PROBLEMS, 12 WERE IDENTIFIED BY THE OIG. THE REMAINDER WERE IDENTIFIED BY SSA AND THE U.S. GENERAL ACCOUNTING OFFICE. WE ARE PLEASED TO POINT OUT THAT 20 OF THESE PROBLEMS HAVE BEEN CORRECTED. WE WILL CONTINUE TO WORK WITH SSA TOWARDS RESOLVING THE REMAINING PROBLEMS, WHICH INCLUDE THE FOLLOWING:

- INDIVIDUAL FIELD OFFICE EMPLOYEES CONTROL ALL OF THE KEY ASPECTS OF PROCESSING A BENEFIT CLAIM. THIS LACK OF SEPARATION OF DUTIES AFFECTS SSA'S ABILITY TO DETECT OR PREVENT FRAUD;
- INADEQUATE CONTROLS OVER RECORDING THE RESULTS OF THE RECONCILIATION OF DIFFERENCES IN WAGE AMOUNTS REPORTED BY EMPLOYERS TO SSA AND THE INTERNAL REVENUE SERVICE;
- WEAKNESSES IN SSA'S AUTOMATED SYSTEMS WHICH CONTROL AND ACCOUNT FOR OVERPAYMENTS MADE TO BENEFICIARIES.

A COMPREHENSIVE LISTING OF OIG UNIMPLEMENTED MANAGEMENT RECOMMENDATIONS, INCLUDING THOSE MADE UNDER FMFIA, CAN BE FOUND IN OUR PROGRAM AND MANAGEMENT IMPROVEMENT RECOMMENDATIONS BOOK, COMMONLY CALLED "THE ORANGE BOOK".

RECOMMENDATIONS

THE SSA HAS COME A LONG WAY IN REDUCING MANY WEAKNESSES. HOWEVER, WE STILL BELIEVE THAT SSA NEEDS TO CONTINUE WORKING ON IMPROVEMENTS IN SSN AND RECORDS ACCESS AND DISCLOSURE. WE MAKE THE FOLLOWING RECOMMENDATIONS, MANY OF WHICH ARE ALREADY BEING ACTED UPON BY SSA:

- DEVELOP PROCEDURES RESTRICTING DISCLOSURE OF INFORMATION TO CALLERS WHO FALSELY IDENTIFY THEMSELVES AS SSA EMPLOYEES OR AS SSN HOLDERS;
- REVISE REGULATIONS ESTABLISHING A ROUTINE USE OF SSN VERIFICATION TO PERMIT SSA TO VERIFY THE SSNs FOR FINANCIAL ENTITIES;
- DEVELOP AND WIDELY DISSEMINATE A SOFTWARE PACKAGE FOR DETECTING INVALID SSN PATTERNS TO ENTITIES THAT ARE NOT PERMITTED ACCESS TO SSA'S AUTOMATED VERIFICATION PROCESS;
- DETERMINE THE FEASIBILITY OF USING PROFILES TO IDENTIFY EMPLOYEES WHO MAY IMPROPERLY USE INFORMATION FROM SSA DATA FILES;

- STRENGTHEN GUIDANCE PROVIDED TO REGIONAL SECURITY STAFFS FOR MONITORING EMPLOYEES FOR POSSIBLE UNAUTHORIZED ACCESS OR DISCLOSURES OF INFORMATION, AND IMPLEMENT RECOMMENDATIONS BASED ON OIG INVESTIGATIVE RESULTS;

- RE-EVALUATE THE CONTINUED DISCLOSURE OF INFORMATION TO PRIVATE PARTIES UNDER CONTRACTUAL AGREEMENTS, AND DETERMINE WHAT ADDITIONAL CONTROLS MIGHT BE IMPLEMENTED TO PREVENT UNAUTHORIZED ACCESS UNDER THOSE AGREEMENTS.

BY WAY OF LEGISLATIVE RECOMMENDATIONS, CONGRESS MAY ALSO WISH TO CONSIDER TAKING THE FOLLOWING ACTIONS:

- UPDATE THE SAFEGUARDS OFFERED BY THE COMPUTER SAFEGUARD ACT OF 1987 AND THE PRIVACY ACT OF 1974. CURRENTLY, FEDERAL AGENCIES MUST ESTABLISH A PLAN FOR THE SECURITY AND PRIVACY OF THEIR COMPUTER SYSTEMS TO PROTECT AGAINST LOSS, MISUSE, OR UNAUTHORIZED ACCESS TO OR DISCLOSURE OF THE INFORMATION CONTAINED IN THESE SYSTEMS. TOUGHER PROVISIONS ARE NEEDED THAT SPECIFICALLY TARGET THE FRAUD POTENTIAL OF CURRENT TECHNOLOGIES.

- TAKE ACTION TO STRIKE A BALANCE BETWEEN THE NEED FOR EXPEDITED IMMIGRATION PROCESSING AND THE INVOLVEMENT OF THE INS IN THE SSN ISSUANCE PROCESS TO ENSURE THE INTEGRITY OF SSN ASSIGNMENTS TO ALIENS.

CONCLUSION

IMPROPER ACCESS TO AND RELEASE OF CONFIDENTIAL GOVERNMENT INFORMATION IS NOT A PROBLEM UNIQUE TO SSA. THE GROWTH OF ALL LARGE DATABASES WITH INCREASINGLY SENSITIVE INFORMATION MAKES FRAUD DETECTION AND PREVENTION ESSENTIAL. NEW SAFEGUARDS NEED TO BE DEVELOPED TO PROTECT ACCESSIBLE DATA BASES.

THE OIG AND SSA ARE BOTH DEEPLY CONCERNED ABOUT THE INTEGRITY OF THIS INFORMATION AND WILL CONTINUE TO VIGOROUSLY INVESTIGATE ANY INDIVIDUALS WHO COMPROMISE THE PUBLIC'S RIGHT TO PRIVACY.

Appendix A
OIG REPORTS ON SSN AND RELATED ISSUES

1. The Social Security Administration Needs to Improve Procedures in its Death Match Operation - February 1992, Control Number: A-13-90-00046.

2. Birth Certificate Fraud Update: A Management Advisory Report - November 1991, Control Number: OEI-02-91-01530

3. Review of the Social Security Administration's Field Office Internal Controls - November 1991, Control Number: A-13-91-00302.

4. Project Clean Data: A Management Advisory Report - February 1991, Control Number: OEI-12-90-02360

5. Suspended Payments Need to be Resolved Timely - September 1990, Control Number: A-13-89-00027

6. Social Security Numbers for Noncitizens - August 1990, Control Number: OEI-05-88-01060.

7. Separation of Duties in the Social Security Administration's Modernized Claims System - February 1990, Control Number A-13-89-00025.

8. Extent of Social Security Number Discrepancies - February 1990, Control Number: OEI-06-89-01120.

9. Social Security Administration, Systems Software Internal Control Review - October 1988, Control Number: A-13-88-00011

10. Extent of Use of Social Security Numbers - August 1988, Control Number: OAI-06-88-00800.

11. Birth Certificate Fraud - March 1988, Control Number: OAI-02-86-00001

12. Controls Over the SSN Application Process - May 1987, Control Number: OAI-05-86-00027.

Prepared Statement Senator Daniel Patrick Moynihan

We meet this morning for an oversight hearing of the Subcommittee on Social Security and Family Policy for the purpose of hearing testimony on an investigation into alleged widespread theft and sale of personal and private records maintained by the Social Security Administration.

We are deeply disturbed by what has occurred. Private firms, so-called "information brokers", have allegedly bribed Social Security Administration employees to steal personal records of individuals from SSA computers for the purpose of selling the information to interested buyers. Such buyers apparently include private investigators, prospective employers, lawyers, insurance companies, and others interested in obtaining, for whatever purpose, someone else's Social Security number and employment and earnings history.

The results of the investigation to date are all the more disturbing because the scam does not appear to be an isolated case, or limited to a particular part of the country. The FBI has arrested at least 18 people in 10 states in connection with the investigation, and Social Security Administration employees in four states have recently been indicted.

One company in Tampa, Florida was so bold as to send out promotional brochures that boasted instant access to confidential computer data on virtually anyone in the country. One such brochure came into the hands of investigators in the Atlanta regional office of the Inspector General of the Department of Health and Human Services. These investigators, together with the FBI, commenced one of the government's most concerted efforts to date to crack down on the newly emerging information broker industry. The investigation appears to involve the largest case ever of theft from government computer files, and may well involve the most serious threat to individual privacy in modern times.

Throughout the history of the Social Security program we have sought to ensure the absolute privacy and confidentiality of the personal information maintained by the Social Security Administration. This agency maintains records on 200 million Americans. This information includes a person's Social Security number, full name, place of birth, date of birth, names of both parents, names of current and past employers, and a complete earnings history. It is of the utmost importance that we keep the promise made over a half century ago to keep this personal information private to the maximum extent possible.

We will hear today from Mr. Larry D. Morey, Deputy Inspector General for Investigations, Department of Health and Human Services, on the status of their on-going investigation into this matter and on any recommendations they may have on how to prevent this kind of violation of people's privacy in the future. We will also hear from Mr. Louis D. Enoff of the Social Security Administration on the kinds of safeguards the agency currently employs to prevent the theft of private information, and on what steps they plan to take in light of the results of this investigation.

Finally, we will hear testimony from a panel of witnesses who are experts on issues of privacy and computer technology. These witnesses include Mr. Morton Halperin of the American Civil Liberties Union, Mr. Evan Hendricks, Chairman of the United States Privacy Council, and Mr. Marc Rotenberg of Computer Professionals for Social Responsibility. We have asked these witnesses to provide us with their insights into the issues raised by this scandal, and to also address the question of whether we need any statutory controls on the use of the Social Security number in the private sector. At present, the use of the Social Security number in the private sector is virtually unregulated. Individuals must provide their Social Security numbers to get bank accounts, insurance policies, credit cards, and any number of things. This fact explains the very existence of information brokers, and it is perhaps past time to look into this matter as well.

PREPARED STATEMENT OF MARC ROTENBERG

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to testify today on privacy protection for social security records and the special problems of the Social Security Number (SSN). My name is Marc Rotenberg and I am the director of the Washington Office of Computer Professionals for Social Responsibility (CPSR). I am also the chairman of the Scientific Freedom and Human Rights Committee of the Association for Computing Machinery (ACM).

CPSR is a national membership organization of computer scientists from across the country. Our membership includes a Nobel laureate and four winners of the Turing Award, the highest honor in computer science. CPSR has a particular interest in privacy issues and we have testified before several Congressional committees in support of efforts to protect privacy.[1] A little over two years ago we completed a report on the proposed expansion of the FBI's computerized record-keeping system at the request of

---

[1] See The Privacy for Consumers and Workers Act Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor and Human Resources, 102d Cong., 1st Sess. ___ (Sept. 24, 1991); The Fair Credit Reporting Act Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs, 102d Cong., 1st Sess. ___ (June 6, 1991); Telemarketing/Privacy Issues Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce, 102d Cong., 1st Sess. 43 (April 24, 1991); Use of Social Security Number as a National Identifier Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991); The Computer Abuse Amendments Act of 1990 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, 101st Cong., 2d Sess. ___ (July 31, 1990); Data Protection, Computers, and Changing Information Practices Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations, 101st Cong., 2d Sess. 109 (May 16, 1990); The Government Printing Office Improvement Act of 1990 Before the Subcomm. on Procurement and Printing of the House Comm. on House Administration, 101st Cong., 2d Sess. 104 (March 8, 1990); Computer Virus Legislation Before the the Subcomm. on Criminal Justice of the House Comm. on the Judiciary, 101st Cong., 1st Sess. 25 (November 8, 1989); Military and Security Control of Computer Security Before the Subcomm. on Legislation and National Security of the House Comm. on Government Operations, 101st Cong., 1st Sess. 80 (May 4, 1989).

Mr. Don Edwards, the Chairman of the Subcommittee on Constitutional and Civil Rights of the House Judiciary Committee.[2]

The ACM is largest association of computing professionals in the United States. It was established in 1947 "to advance the sciences and art of information processing; to promote the free interchange of information about the sciences and arts of information processing both among specialists and among the public; and to develop and maintain the integrity and competence of individuals engaged in the practice of information processing." The Scientific Freedom and Human Rights Committee has the special responsibility to oversee those computing activities that may adversely impact individual freedom and human rights.[3]

---

[2] FBI Oversight and Authorization Request for Fiscal Year 1990 Before the Subcomm.on Civil and Constitutional Rights of the House Comm. on the Judiciary, 101st Cong., 1st Sess. 512 (May 18, 1989).

[3] The ACM has a long-standing commitment to privacy protection. The ACM Code of Professional Conduct states that:

> An ACM member should consider the health, privacy and general welfare of the public in the performance of the member's work. (E.C. 5.1)
>
> An ACM member, whenever dealing with data concerning individuals, shall always consider the principles of individual privacy and seek the following: To minimize the data collected; To limit authorized access to the data; To provide proper security for the data; To determine the required retention period of the data; and to ensure proper disposal of the data. (E.C. 5.2).

A year ago the ACM passed a new resolution, reaffirming its support for privacy protection. The resolution stated that:

> Whereas the ACM greatly values the right of individual privacy;
>
> Whereas members of the computing profession have a special responsibility to ensure that computing systems do not diminish individual privacy;
>
> Whereas the ACM's Code of Professional Conduct places a responsibility on ACM members to protect individual privacy; and
>
> Whereas the Code of Fair Information Practices places a similar responsibility on data holders to ensure that personal information is accurate, complete, and reliable;
>
> Therefore, be it resolved that
>
> (1) The ACM urges members to observe the privacy guidelines contained in the ACM Code of Professional Conduct;

INFORMATION BROKERS BUY AND SELL CONFIDENTIAL GOVERNMENT RECORDS

Two months ago, The Washington Post reported that 16 individuals in 10 states were arrested in the largest case ever involving the theft of federal computer data. So-called information brokers boasted that they could provide detailed personal information on anyone in the country. The records ranged from private credit reports and business histories to driver's license records, Social Security records and even criminal history history backgrounds. These confidential records were taken from government agencies and then sold for a fee to lawyers, insurance companies, private employers and others. Peter Neumann, a computer security expert, said that "The public is abysmally uninformed about problems like this. With sufficient access to a few databases these days, you can get pretty close to somebody's life history with nothing more than a Social Security Number."[4]

A story in Time magazine described a "black market in government data" that included Social Security employees, police officers, private eyes and "information brokers." According to Time, Social Security employees sold earnings histories for $25 apiece, and these were then marked up and resold by brokers for as much as $175. Even a top-ranked IRS criminal investigator was recently indicted for selling non-public marital records to a California-based investigation outfit run by ex-IRS officials.[5]

SIGNIFICANCE OF GROWING RECORD PROTECTION PROBLEM

The first reaction to these stories might be to call for more prosecutions or new criminal penalties for the sale of personal information. Both measures might be considered, but neither

---

(2) The ACM affirms its support for the Code of Fair Information Practices and urges its observance by all organizations that collect personal information; and

(3) The ACM supports the establishment of a proactive governmental privacy protection mechanism in those countries that do not currently have such mechanisms, including the United States, that would ensure individual privacy safeguards.

[4] Michael Isikoff, "Theft of U.S. Data Seen as Growing Threat to Privacy," The Washington Post, December 28, 1991, at A1.

[5] Richard Behar, "Psst, Secrets for Sal: Shady Dealers are doing brisk trade in IRS, FBI and other federal data," Time, February 24, 1992.

approach is likely to address the fundamental changes that must be taken in the next few years to ensure the privacy of personal information held by federal agencies.

To understand the extent of the problem with the protection of records held by the Social Security Agency and the special problem of the social Security number, it is helpful to look at a sales brochure of Nationwide Electronic Tracking, which the FBI believes was at the center of this operation. According to that brochure, with just a person's Social Security Number, Nationwide Electronic Tracking could provide name and home address (with 1-2 hours for $7.50), place of current employment (1 week, $75), and previous employment and earnings (3-5 days, $100-$175).[6]

Now it may be possible to crack down on information brokers such as Nationwide Electronic Tracking, but what should be done over long-term about the many other holes in the government's record-keeping systems, such as the IRS's careless practice of printing social security numbers of the mailing labels for the form 1040s?[7]

A long range solution for the privacy protection of Social Security records, and similar government records, will require looking more closely at the need to control the use of the Social Security number and to establish an independent agency charged with privacy protection.

THE PRIVACY ACT SOUGHT TO CONTROL THE MISUSE OF THE SSN

In 1973 an expert panel of computer scientists, business leaders, civil libertarians, and government officials undertook a study, at the request of then HEW Secretary Elliot Richardson, on

---

[6] The text of the brochure appears in the current issue of Harper's Magazine at 26 (March 1992).

[7] Dr. Willis Ware, the chairman Federal Computer and Privacy Advisory Board, is unequivocal is his assessment of the IRS practice of displaying the SSN on a mailing label. He said:

> I regard the IRS's inclusion of SSNs on tax-form mailing labels as a risky and careless practice that has the effect of unwarranted and needless disclosure of sensitive personal data to casual or potentially malicious eyes. Granted the essential utility of the SSN to improve the accuracy of IRS record-keeping, there are certainly means for concealing a portion of the label from sight and maintaining the confidentiality of the SSN.

Ingerman v. IRS, No. 91-5467, at 13 (Third Circuit 1991) (Brief amicus curia of CPSR).

the potential problems with automated data processing systems. That study produced a landmark report Records, Computers, and the Rights and the Rights of Citizens which became the foundation for the Privacy Act of 1974. Among the issues considered in the study was the potential misuse of the SSN. On this matter, the Advisory Committee was very clear. It stated that:

> We recommend against the adoption of any nationwide, standard personal, identification format, with or without SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government or government-supported automated personal data systems.

The Advisory Committee further recommended that:

- Use of the Social Security Number be limited to only those purposes required by the federal government
- Federal agencies should not require the use of the Social Security number without statutory authority.
- Congress should evaluate any proposed use of the Social Security Number
- Individuals should have the right to refuse to provide their Social Security Numbers, and should suffer no harm for exercising this right.
- Organization required by Federal law to obtain the Social Security Number use the number solely for the purpose for which it was obtained and not make any secondary use of disclose the Number without the informed consent of the individual.

In 1974 Congress adopted many of the recommendation of the Advisory Committee and made clear that the use of the Social Security Number would be restricted. Section seven of the Privacy Act of 1974 said specifically that:

> It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (7)(a)(1).

The Privacy Act further stated that:

> Any Federal, State or local government agency which requests an individual to disclose his social security number shall that individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what use will be made of it. (7)(b)

This means that any government agency which requests an individual's social security number is required to (1) cite its formal legal authority for using the number; (2) reveal whether disclosure is mandatory or voluntary; and (3) explain how the number will be used.

Mr. Chairman, these are very good principles and the provisions set out in the Privacy Act could go a long way toward controlling the misuse of the SSN. They reflect the widespread belief that the development of a single universal identifier would lead to a personal privacy and might encourage anti-democratic tendencies.

MISUSE OF THE SSN BY THE PRIVATE SECTOR HAS CREATED NEW PROBLEMS

Richard Kusserow, the Inspector General of the Department of Health and Human Services, recently wrote that as the use of the SSN "as an identifier has grown, so has the opportunity for misuse."[8] Stories across the country during the past year demonstrate that the incidents of SSN fraud is on the rise. One story revealed that the are more than 300 fraud incidents involving social security numbers every year in Massachusetts. According to the Boston Globe:

> Because the state uses the Social Security numbers as license numbers, the theft of a license gives a thief access to another person's name, address and social security number. Authorities say that, with another person's Social Security number, a thief can apply to obtain that person's welfare benefits, Social Security benefits, credit cards or even the victim's paycheck.[9]

An article from a California paper reports that the rate of Social Security fraud is dramatically increasing, from 390 cases in 1988 to an estimated 800 cases in 1991. According to the article, "experts attribute the increasing abuse of the Social Security number to two factors: undocumented immigrants seeking

---

[8] "How We Fight Waste: Report from the Inspector General of HHS," Government WasteWatch, at 17 (Winter 1992).

[9] Elizabeth Neuffer, "Victims urge crackdown on identity theft: Say officials often fail to act on complaints," The Boston Globe, July 9, 1991.

work in the United States, and the business world's increasing use of the number as a universal ID."[10]

In another incident with almost Orwellian implications, a college student was arrested by campus police when he failed to provide his social security number, after he had given the officer his name and address.[11]

THE UNRESTRICTED USE OF THE SOCIAL SECURITY NUMBER UNDERMINES PRIVACY AND IT IS AN INHERENTLY FLAWED IDENTIFIER

The central privacy problem with the use of a Social Security Number as an identifier is that it allows organizations to compile information about individuals without their knowledge or consent. This tends to diminish an individual's ability to control information about himself or herself and leads to the compilation of elaborate dossiers.

When an individual discloses an account number to a particular business or institution, the information that is disclosed is only that necessary to identify the person to the particular institution. The disclosure of personal information to a particular company for a specific purpose establishes an expectation of confidentiality.[12] Numbering schemes that are designed for particular businesses help promote confidentiality because they strengthen the ties between the individual and the institution and create an expectation that information which is transferred to the institution will not be used for other purposes.

Similarly, single-purpose identification schemes without universal identifiers can actually enhance personal privacy by restricting the extent of a person's identity that must be disclosed to interact with a large institution. A typical library card is a good example. In those information systems, privacy protection should focus on the subsequent use of the information by the information-holding institution, but the card by itself is unlikely to create a privacy problem.

---

10 Yasmin Anwar, "Thieves Hit Social Security Numbers: Fouled Up Benefits and Credits," San Francisco Chronicle, August 30, 1991, at 1.

11 Chris Hawley, "State dismisses charge in bicycle-moving case," Bowling Green News, November 21, 1991.

12 Report of the Privacy Protection Study Commission (1977).

Multi-purpose identification numbers for which the purpose is open-ended may be more problematic. An institution that obtains the number presumably will have access to all the information that the document holder would have. This access allows the institution to create more elaborate picture of the document-holder than the single-purpose document.

From a design standpoint there are a number of reasons that the growing use of Social Security Numbers will lead to greater problems, errors in record-keeping as well as fraud. First, the SSN is an imperfect identifier. It is not unique for each individual, and there are many reported cases of misidentification

There is also a particular problem where the SSN is used an "authenticator" or password as some organizations have tried to do. This would be similar to placing a three-digit combination lock on a locker with a three-digit designation, such as "215," and then setting the number on the combination lock to correspond with the number on the locker. Any person who could read the number on the locker door could open the combination lock.

But even if a perfect identifier were developed, perhaps stamped on a bracelet that each person would wear, the privacy problems would remain. In general the SSN promotes the unanticipated transfer of personal information. As CPSR member and computer researcher Chris Hibbert has noted "Multiple record systems keyed to the same identifier make it difficult to restrict the release of personal information to selected institutions and encourage compromise."

ALTERNATIVES TO THE SSN EXIST

It is a truism in the privacy world that the SSN has become a "de facto national identifier" as if there were no alternative to placing a nine-digit code on every record containing personal information or that this particular problem was some how beyond our ability to solve. In fact, every day organization make decisions about the design of record systems and whether the use of the SSN as an identifier is necessary or appropriate. While some industries, such as the Associated Credit Bureaus, rush to databases of detailed personal files using the SSN, other organizations avoid the SSN and develop their own, oftentimes more accurate, numbering scheme. Similarly at the state level, some states have placed an unnecessary reliance on the SSN while other states have developed better policies.

In one striking case, a resident in the state of Virginia was denied the right to vote because he would not provide his Social Security number to the State Board of Elections. He was, in every other way, eligible to vote. However, he could vote in Virginia because Virginia is one of the few states in the country

that makes disclosure of the SSN a mandatory registration requirement.[13]

Why should Virginia impose this requirement? Few of the other states do. In another area of state administration, motor vehicle records, the state of Maryland just this week took an important step in the right direction when the Motor Vehicle Administration announced that it "will stop requiring applicants to divulge their Social Security numbers when obtaining or renewing driver's licenses." According to an article in yesterday's Washington Post, Maryland does not print Social Security numbers on driver's licenses. The agency will continue to ask for the number, but applicants will not be required to provide it.[14]

This is clearly a welcome development. Similarly, other states have taken steps to control the collection and use of the SSN. There does seem to be a growing awareness of the potential for abuse, and a willingness to consider safeguards and alternatives.

The point, Mr. Chairman, is that whether the SSN is requested and used in a system of records is ultimately a question of public policy that can be decided in the Congress or the state legislatures. It is not a problem beyond control.

There is further reason to be hopeful about this problem. A computer researcher named David Chaum has proposed a method that could protect security and privacy for individuals while providing businesses and agencies with the information they need for commercial transactions and user authentication.[15] Dr. Chaum's work has attracted a great deal of interest in the computer science community. If he has found a successful way to permit commercial transactions while controlling the undesired secondary transfer of personal information, then a great breakthrough may be at hand. To use an analogy from the environmental world, this would be similar to designing an engine that generated no pollutants.

---

[13] CPSR is assisting Marc Greidinger in this case. Greidinger v. Davis, No. 91CV00476 (Eastern District of Virginia 1991).

[14] "Around the Region: Md. Forgets the Number," The Washington Post, February 27, 1992, at C6.

[15] David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM (October 1985). An abridged version of Mr. Chaum's research appears in the proceedings of the 1991 Cryptography and Privacy Conference sponsored by CPSR, the Electronic Frontier Foundation, and RSA Data Security in Washington, DC. "Numbers Can Be a Betyter Form of Cash than Paper

RECOMMENDATIONS

Mr. Chairman, we are very pleased that you have convened this hearing to look at the problem of privacy protection for Social Security records and the special difficulties with the widespread use of the SSN. Certainly, one response could be to encourage more raids, to strengthen criminal fines, and to monitor government workers more closely. But, given the dramatic changes currently underway and the need for a long-term solution, we would propose the following steps.

First, CPSR strongly supports the establishment of a data protection board in the United States and recommends that you support the proposal which has been introduced in the House by Congressman Bob Wise. These new privacy problems are far-reaching and complex. Agencies are trying to address privacy concerns, but oftentimes they lack the resources or the expertise to to develop appropriate solutions. Many countries have established independent data protection agencies precisely to fill this function. In fact, the creation of independent oversight agency was considered a critical component of the Privacy Act of 1974. Regrettably, this provision was removed prior to passage of the Act. (I have attached to my testimony as article that describes the proposal in more detail).

Second, CPSR recommends that the Privacy Act restrictions which control the misuse of the SSN by the public sector be extended to the private sector. No company should request a Social Security without explicit statutory authority. Where the number is necessary for tax reporting purposes, then the company must take measures to ensure that it is not improperly disclosed. Fines and sanctions should be imposed when companies obtain the SSN without authority or publish the SSN without consent.

Third, CPSR recommends that either the Computer Science and Telecommunications Board of the National Research Council or the Office of Technology Assessment undertake a study of alternative information transaction schemes, such as the one proposed by David Chaum, for record-keeping systems. The purpose of such a study would be to determine how best to achieve the twin goals of protecting privacy for the individual and ensuring the transfer of necessary information for the institution.[16]

---

[16] Both the NRC and OTA have recently completed studies in related areas. In 1991 the CSTB released Computers at Risk: Safe Computing in the Information Age which set out a series of important policy recommendation for computer security. In 1987 the OTA completed Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.

Mr. Chairman, certainly these are strong measures. Many organizations in the private sector rely on the SSN for records management and will be reluctant to change. However as more organizations turn to the SSN, the incidents of fraud will increase and the opportunities for misuse will multiply. A far-reaching problem will require a far-reaching solutions.

A little more than twenty years ago MIT President Jerome Weisner testified before Senator Sam Ervin's Committee on the need for strong privacy measures. Professor Weisner drew an parallel between the challenge of privacy protection and public policy in the area of environmental protection. He stated that:

> It is obvious that means for effective record-keeping, information gathering, and data processing are essential needs of a modern society. The problem for us is to determine how to reap the maximum assistance from modern technology in running a better society and at the same time, how to keep it from dominating us. In order to do this we may need to adopt some stern measures in the form of very strict controls on who can do what with private information about any individual in the society.[17]

This concludes my testimony. I would be pleased to answer your questions.

---

[17] "Federal Data Banks, Computers and the Bill of Rights," Senate Judiciary Committee (1971).

In Support of a Data Protection Board in the United States

Marc Rotenberg*

The development of commercial products containing detailed compilations of personal information underscores the need for the establishment of a Data Protection Board in the United States. Computer technology facilitates the exchange of personal information, but responsibility for the proper use of personal data lies with the organization that collects the information. Whereas other countries have moved aggressively to establish reasonable safeguards to protect individual privacy through the creation of data protection boards and privacy commissions, the United States has failed to adopt similar measures. A privacy protection commission was a key component of the original privacy protection scheme developed by the Congress in the early 1970s but was never enacted. Recent public polling data suggests that the creation of a similar board today would be supported by a wide majority of Americans.

The United States must move quickly to address the growing privacy problems that arise from the collection and transfer of personal information generated by computerized recordkeeping systems. Failure to do so will likely increase public concern about privacy safeguards and undermine efforts to develop new products that are technology based.

Automated information systems, by virtue of their processing capability, pose an ongoing risk to personal privacy. For this reason, the computer science community has long argued that adequate safeguards must be established to protect personal information. The code of ethics of many computer associations and related professional organizations clearly state the importance of data protection in the design of computer systems.[1] Computer scientists have also played a prominent role in congressional proceedings and the development of key reports that gave rise to many of the privacy laws in the United States today.[2] And computer privacy remains a central concern at regular meetings of computer professionals.[3]

Goverment Information Quarterly, Volume 8, Number 1, pages 79–93.
 ISSN: 0740-624X.

The Computer Professionals for Social Responsibility (CPSR) has played a leading role in recent efforts to develop appropriate privacy safeguards. In 1986, CPSR established a special project on computer and civil liberties to address growing concern among our membership about privacy safeguards. Since that time we have reviewed the privacy and civil liberties implications of various computing systems in both the public and private sector, and have recommended appropriate safeguards.[4] Two years ago, several of our members participated in an expert panel review of the proposed expansion of the FBI's records system at the request of Congressman Don Edwards.[5] That review led to the decision to drop a proposed tracking feature that could have turned the FBI's database into a national surveillance system.[6]

Concerns about privacy protection are widely shared by the general public. Opinion polls and research studies have consistently shown that Americans are concerned about the protection of privacy and will support legislative efforts to protect privacy.[7] In recognition of this concern, many large organizations in both government and the private sector have developed policies and practices to safeguard personal information.[8]

Though the courts and the Congress have struggled to define the right to privacy, there can be little doubt that such a right is necessary for the protection of individual liberty that makes democratic self-governance possible. Without the ability to control the disclosure of the intimate facts, individuals lose the ability to shape identity, to establish trusts, and to form smaller communities within the larger community. It is not a coincidence that a primary attribute of totalitarian societies and the dystopias that are often found in science fiction is that individuals lack personal privacy.

Privacy is the right of individuals to control the disclosure of personal information and to hold those accountable who misuse information, breach a confidence, or who profit from the sale of information without first obtaining the consent of the individual. In the design of a computer system containing personal information, it is a primary consideration.

There is little question that new computer technology has made it easier for large organizations to collect and exchange information about individuals.[9] And it has also made possible inferences about individual behavior based on this information. Computer technology has spawned an enormous proliferation of detailed transactional data that can be used for purposes potentially detrimental to the interests of the person involved. The problem today is that there is inadequate policy guidance to ensure the protection of privacy for this personal information.

For example, a simple billing statement sent by the phone company to verify the monthly charges provides a readily accessible list of all the people contacted, the length of the calls, and the location of the calls. For the phone subscriber this information is important to verify charges. To an unknown third part, it would provide a window into the subscriber's personal life, a listing of friends and associates, an invasion of privacy more intrusive than if a stranger were to leaf through a personal address book copying down the names and numbers.[10] While phone companies have traditionally safeguarded this information,[11] there is a growing awareness that the traditional restrictions are being relaxed. Certain phone services, such as 800 phone services, are now developed specifically for the purpose of gathering marketing data.

The problem is further compounded when transactional data from different sources are gathered in a single place to create a detailed dossier of spending habits, political associa-

tions. :ends and neighbors, lifestyle, and work hours. Few people would willingly consent to the development of the electronic profiles that are now becoming available. However, because the United States has failed to establish enforceable rights for privacy protection for this transactional data, detailed information is now available for sale without the knowledge or consent of the person described.

Computer scientists working with policy makers anticipated many of the privacy problems that could result from the unrestricted use of transactional data. In 1973, they helped to draft a set of principles—The Code of Fair Information Practices—that were designed to minimize the privacy risks of automated systems containing personal information. The Code set out a series of principles for the protection of personal information stored in computer systems.[12] These principles are:

- There must be no personal data recordkeeping systems whose very existence is secret;
- A person should know what information about that person is in a record and how it is used;
- A person should be able to correct or amend a record of identifiable information about the person;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data; and, most importantly,
- Any information obtained for one purpose should not be used for another purpose without the consent of the person.

This last principle is the cornerstone of the Code and the golden thread that ties together virtually all of the data protection law in the United States.[13] It is based on a simple premise: that when you give personal information for a particular purpose—to obtain a warranty, to reserve a hotel room, or to charge a dinner—you do not reasonably expect that the information will be used for another purpose without your consent. That is the implied promise between you and the institution. When the institution breaks that trust, they have undermined your expectation of privacy and acted without regard to your interest in controlling records of your personal life.

There has been a great deal of public interest in the "frequent shopper" programs.[14] These are programs that allow supermarkets to collect detailed information on particular customers. The computer in combination with point of sale (POS) scanning technology, makes it economically feasible to collect and analyze a great deal of transactional information that previously would have been impossible to gather. A supermarket manager can now tell that a particular customer buys broccoli and not asparagus, prefers frozen vegetables to canned vegetables, and possibly whether that customer buys contraceptives, antidepressant drugs, or tabloid magazines.

From the seller's viewpoint this could be a wonderful innovation. Sellers have far more information about the preferences of their customers. They can make purchasing decisions more effectively. They can target products to particular customers based on buying patterns. For example, the store might offer rebates to customers who buy four cans of a specific brand of coffee over three months, or the seller might reward buyers who frequently return to the store with discounts and bonuses, similar to the mileage programs

offered by the airlines. For the effective manager, the frequent shopper program should produce larger sales, greater revenue, and increased customer loyalty.

From the customer's viewpoint, as well, the program may also produce benefits—products more carefully tailored to particular needs, better value, and more efficient services. Customers will find that their supermarket is recommending specific products based on their buying habits. For example, frequent buyers of frozen dinners are likely to receive special offers for new frozen dinner products. The image that comes to mind is that of the corner store where the shopkeeper, knowing that you like a particular item, smiles as you enter the store and pulls out from beyond the counter a jar of pickling sauce that you always try to find and that is often out of stock.

The problem with the frequent shopper program is that it is not just the shopkeeper in the corner store that knows of your preference of a certain pickling sauce. Under the programs currently underway, the personal data gathered at local supermarkets will flow into the computers of Citicorp. Citicorp will also know who likes pickling sauce, who has hemorrhoids, and who buys condoms. And here is the problem. Why should one of the country's largest financial institutions also become a broker for the shopping preferences of American customers? And why should they obtain this information without the knowledge and informed consent of consumers?[15]

Of course, Citicorp is not alone in the efforts to sell personal data. An extraordinary product, due out on the market in 1990, is Lotus MarketPlace. MarketPlace is a CD-ROM—a computer disk—containing the buying preferences of 80 million American households. The disk contains profiles on 120 million American consumers, including:

- Name;
- Address;
- Age;
- Gender;
- Marital status;
- Household income;
- Lifestyle;
- Dwelling type, and
- Actual buying habits across 100 product catagories.[16]

From a data protection viewpoint, this product would receive low scores. First, the product violates Fair Information Practices—personal information which was collected for one purpose is used for another purpose without the individual's consent. It is fair to say that very few of the 120 million people listed in MarketPlace consented to the use of their personal information in this way. And though Equifax has claimed that it is not possible to obtain information on specific individuals—only lists—it is hard to understand why it would not be possible to extract highly detailed information about individuals. In fact, Equifax is already using their in-house databases in precisely this way for screening potential employees.[17]

There is currently no legal safeguard that prevents Equifax from selling individually identifiable information to third parties if it chose to. This is a critical privacy concern for the American public and Congress.

Second, CD-ROM is a read-only medium, which is to say that once the information is

stored it cannot be erased. There is no effective mechanism for consumers to "opt-out" of the list once the CD-ROM are distributed. And there is no way to correct data inaccuracies once the product hits the streets. With such a readily available and extensive compilation of data from different sources, the product takes computer matching to a new level. Not surprisingly, Equifax has stated that it has no plans to notify individuals or inform the public that they will be marketing this data.[18]

This new product poses a particular threat to personal privacy because it places the actual data in the hand of individuals and beyond the control of even the responsible information brokers. Those who purchase MarketPlace may not follow the Direct Marketing Association's guidelines for personal information protection and ethical mailing list practices. Further, there is no guarantee that these individuals or organizations will not ultimately be able to access all the identifiable information on the disk. There is nothing to prevent other firms from selling similar products with even more detailed information on individuals.

Once this information on lifestyles and buying habits is sold to third parties, the ability to control the disclosure of personal information is diminished and the right to privacy is undermined.

These companies should not sell information about any consumer without first obtaining consent and then taking adequate steps to ensure that the data are accurate, complete, and timely. If they fail to do this, then consumers who value their privacy should write to Citicorp and Equifax, sending copies of their letters to this committee, their elected representatives, and the U.S. Office of Consumer Affairs, objecting to the sale of this product.

There are other information products which clearly undermine privacy, are at odds with principles of data protection, and would be opposed if more widely known. For example,

- Philip Morris, as part of its promotion for the Bill of Rights, solicited home telephone numbers from all individuals who called to request a copy of the Bill of Rights. But telephone number are not needed to mail a copy of the Bill of Rights, the alleged purpose of the promotion. However, telephone numbers do serve as a vital link to other databases which Philip Morris might search to learn more about the demographics and lifestyles of individuals responding to the promotion.[19]
- Wats Marketing of Omaha, Nebraska has 10,000 incoming 800 number phone lines with Automatic Number Identification connected to Donnelly Marketing's Fast Data System. According to a recent issue of *The Friday Report*, a direct marketing trade newsletter, the phone numbers of incoming calls will be matched with the home addresses of more than 80 million individuals in the Donnelly database. As a result, individuals who make an anonymous phone call to an 800 phone number to request information will find themselves the unwitting target for subsequent mailings and telemarketing campaigns. Even the fact that these people responded to a campaign for a particular product or service will be sold to anyone interested in targeting individuals who use the phone to shop.[20]
- Large mailing list brokers routinely merge single lists they manage with demographic or lifestyle information. For example, Worldata recently advertised, "the Holiday Inn Great Rates List," identifying the list members as adults, ages 25 to 45, heading families with an average household income of over $30,000 who have responded to

print or television advertisements for Holiday Inn.[21] It is unlikely that the individuals on the Worldata list who responded for the Holiday Inn ads provided all this detailed information, nor expected that responding to an ad would mean that third parties would obtain such detailed personal information.

- Most disturbing, hospitals are now selling medical information for direct marketing. Hospitals have also learned that they can generate lists by sponsoring seminars, fairs, or health-screenings at a shopping mall or exposition. The hospital then uses the names of the persons who register for the free seminar and follows up with mailings or telephone calls soliciting business for the hospital.[22]

The firms which collect and sell this information argue that there is no real harm and that consumers benefit from these practices. But if the companies were required to tell consumers how this information was obtained and were then required to seek consent before the information was resold, they would have a far more difficult time justifying the sale of these elaborate dossiers.

What is taking place is . orm of deception cloaked under the banner of innovation. Detailed personal information—age, gender, marital status, and income—is being bought and sold with little regard to the long-term implications for personal privacy or the concerns of the American people. The companies that engage in these practices say do not worry, it is all to your benefit, there is no need for government review.

It is hard to believe that this response would satisfy most Americans. According to a recent privacy survey:

- 90% of all Americans do not think that companies disclose enough information about their list usage; and
- 80% do not think companies should give out personal information to other companies.[23]

Not surprisingly, much of the most informed concern about the privacy implications of these new practices is coming from within the direct marketing industry, from the people who are most familiar with the data collection practices and recognize the privacy dangers. For example, the editorial director of *Target Marketing Magazine* wrote recently:

> The issue of consumer privacy will not go away simply because direct marketers don't confront it. . . . The privacy question is really about trafficking in information that is freely obtained for one purpose and then sold for another. When a consumer fills out a credit application, because he must do so in order to obtain a credit card, does he understand that this information will be traded, rented and sold? Is he given an option of whether or not that information may be revealed to others? Do lifestyle questionnaires include options as to whether or not that information may be revealed to marketers? . . . We must give consumers these options. They must be presented as positive options . . . not negative ones. This industry must protect itself. If we don't take the lead and deal with the privacy question, Congress could force us to deal with it on someone else's terms.[24]

There is good reason that market research firms and credit bureaus should be concerned about the adequacy of private safeguards. Another recent poll revealed that marketers and credit bureaus rate lowest for protecting customer confidentiality.[25]

The particular concern of privacy advocates who have studied the effects of automated information systems is the tendency of information systems, absent adequate safeguards, to form enormous pools of personal activities. This problem was recognized by the ranking minority member of the Committee on Government Operations, Representative Frank Horton, who said almost twenty-five years ago:

> One of the most practical of our present safeguards of privacy is the fragmented nature of personal information. It is scattered in little bits across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard.[26]

The problem with these new commercial products that are based on the compilation of personal information is that it is easy to see the benefits and more difficult to assess the costs. This problem was anticipated by Jerome Wiesner, the former dean of MIT and former science Adviser to President Kennedy. Testifying before a Senate subcommittee in 1973, Wiesner warned that, absent adequate safeguards, automated record systems might lead to an "information tyranny":

> Such a depersonalizing state of affairs could occur without overt decisions, without high-level encouragement or support and totally independent of malicious intent. The great danger is that we could become information bound, because each step in the development of an information tyranny appeared to be constructive and useful.[27]

The challenge today is to ensure that such an information tyranny does not result even though each step along that path appears beneficial.

THE UNITED STATES HAS A WELL ESTABLISHED COMMITMENT TO INFORMATION PRIVACY WHICH MUST BE EXTENDED TO PRIVATE SECTOR ACTIVITIES THAT VIOLATE THE CODE OF FAIR INFORMATION PRACTICES

Large organizations in both the government and the private sector have an obligation not to disclose personal information about individuals without the consent of the individual. This was the principle underlying the Privacy Act of 1974 and it is the threat that ties together virtually all of the privacy laws in this country. When an organization discloses personal information without consent, or effectively compels the disclosure of personal information as the cost of doing business, it has diminished the right of privacy, our most fragile freedom.

Privacy protection need not be measured against economic benefit and corporate riches. The equation mistakenly places individual liberty on the auction block. Many companies have developed policies that respect the privacy interests of their customers and their employees.[28] In the computer industry, advertisers frequently use "bingo" cards to allow subscribers to contact manufacturers about product inquiries. It is a good system—the consumer affirmatively indicates, by completing the card, interest in receiving information from the manufacturer. There are other examples of good privacy protection practices, such as phone directories that clearly indicate that the 911 phone service has a call trace feature. In this way, individuals who call a 911 number will have fair notice that the

location of the call will be known to the police. Another example is the NAD (USA) "Non-Warranty Card" which clearly informs the purchaser that the product warranty does not depend on the return of the card and that if the consumer chooses to return the card, the information will be used for marketing research.

Another example of a good privacy practice is the privacy policy adopted by New York Telephone. This is particularly notable at a time when many phone companies are selling transactional data generated by phone calls. New York Telephone has said to its customers:

> It is New York Telephone policy to protect the privacy of your account information. This includes the types, locations and quantity of all services to which you subscribe, how much you use them and your billing records. We will release this information to persons or companies not affiliated with New York Telephone, such as enhanced service vendors, only when you authorize such a release in writing.[29]

These policies help protect privacy interests and should be encouraged. But standing alone they are not sufficient. Too few companies have adopted such privacy policies; too many gather data in a misleading fashion and sell it without obtaining consent. It is for this reason, that Congress must act.

TIME FOR GOVERNMENT ACTION

It is clear that the time has come for Congress to address one of the most pressing issues that will confront this country in this decade—the protection of information privacy. Recognizing that there is widespread support in the United States for new privacy legislation and that current safeguards are inadequate, the question is simply where to begin. The answer is to establish a Data Protection Board. The Board is the missing piece in the privacy protection framework of the United States.

The establishment of a Federal Privacy Board was the cornerstone of legislation introduced by Senator Sam Ervin in 1974. His bill became the Privacy Act, the foundation of privacy protection in the United States. However, strong opposition by the Ford White House led to the demise of the proposed Board before final passage. In its place, a Privacy Protection Study Commission was created.[30]

But when the Commission completed its study of privacy protection in 1977, the same conclusion was reached. The Privacy Protection Study Commission recommended the creation of the Federal Privacy Board. It believed that the Board could play an important role in safeguarding privacy. The final report of the Commission recommended:

> That the President and the Congress should establish an independent entity within the Federal government charged with the responsibility of performing the following functions;
>
> - To monitor and evaluate the implementation of any statutes and regulations enacted pursuant to the recommendations of the Privacy Protection Study Commission, and have the authority to formally participate in any Federal administrative proceedings or process where the action being considered by another agency would have a material effect on the protection of personal privacy, either as the result of direct government action or as a result of government regulation of others.

- To continue research, study, and investigate areas of privacy concern, and in particular, pursuant to the Commission's recommendations, if directed by Congress, to supplement other governmental mechanisms through which citizens could question the propriety of information collected and used by various segments of the public and private sectors.
- To issue interpretative rules that must be followed by Federal agencies in implementing the Privacy Act of 1974 or revisions of this Act as suggested by this Commission. These rules may deal with procedural matters as well as the determinations of what information must be available to individuals or the public at large, but in no instance shall it direct or suggest that information about an individual be withheld from individuals.
- To advise the President and the Congress, government agencies, and, upon request, states, regarding the privacy implications of proposed Federal or state statutes or regulations.[31]

The commission recognized that the board need not have enforcement power over private sector record systems, but that it would have a responsibility to identify privacy abuses and recommended changes. It would, in effect, be an ombudsman, a spokesperson for the widely shared belief of Americans that privacy is cherished value in a free nation and must be considered in the design of computer systems containing personal information.

Thirteen years later, there can be no doubt that the United States needs a Data Protection Board. There is no mechanism to assess the new uses of transactional data. Current privacy safeguards are simply inadequate.

First, individuals now carry the burden for identifying improper data collection practices and making corrections in personal records. When information is shared across the Federal government or between public and private organizations, it becomes increasingly difficult to identify problems and resolve complaints. A single agency would provide valuable assistance.

Second, the Office of Management and Budget (OMB) has failed to fulfill the role of privacy ombudsman, a stop-gap result of the failure to include the Board in the original Privacy Act of 1974. As Flaherty notes in his recent book on data protection in the United States and abroad, OMB has exercised weak leadership.[32] When privacy requirements conflict with other Federal agency goals, there is little guarantee that individual rights will prevail absent oversight from an independent board.[33]

It should be noted that in the past year the Director of the U.S. Office of Consumer Affairs has played an important role in drawing attention to new privacy problems for American consumers. Guiton has been an outspoken advocate in defense of privacy rights and has renewed the long-simmering debate within the United States about the adequacy of current privacy safeguards. At the same time, regrettably, the Office has failed to endorse important privacy measures. Consumer education, industry self-regulation, and voluntary guidelines are not a substitute for enforceable legal rights that guarantee the protection of consumer privacy. Self-help measures, such as opt-out provisions, have placed an onerous burden on consumers. The Office of Consumer Affairs is moving in the right direction, but it must go much further and with more support from the Administration.

Third, the United States lags behind other countries in protecting the privacy rights of

its citizens. Independent privacy boards and commissions were established more than a decade ago in Sweden, France, West Germany, and Canada! As participants in the emerging global economy, American companies are directly affected by data protection laws in other countries. The lack of a data protection agency in the United States leaves U.S. firms unrepresented when decisions are made about the transborder exchange of personal information.[34]

Finally, sector by sector protection of personal information in the private sector has left significant gaps in Federal privacy law. Certain records are covered by Federal statues; other records receive no protection at all. The Computer Matching Act of 1988, designed to prevent the development of computerized dossiers, does not address the widespread exchange of personal information between private sector companies. If a similar record exchange were proposed for Federal agencies, it would be strictly prohibited under the Privacy Act of 1974.

The Data Protection Board could address these activities that undermine well-established privacy standards. The Board could also promote successful industry data protection practices, such as the adoption of Fair Information Practices described by Linowes in *Privacy in America*.[35]

The effectiveness of the board would also be greatly enhanced if the following changes were made. First, the bill should vest the Board with enforcement powers over Federal agencies. Without any enforcement mechanism, such as the power to issue cease and desist orders that was proposed in Senator Ervin's 1974 bill, it is unclear how effective the Board will be.

Second, the size of the Board should be increased and membership terms should be modified. A three-member Board will not be adequate if the Board assumes greater responsibilities in the future. Further, if any of the seats on the three-member Board became vacant, the functioning of the Board will be severely jeopardized. Consistent with the original 1974 proposal, the Board should also be expanded from three to five members, while maintaining the current funding level. The remaining two positions would be funded only as needed in the future. Furthermore, the terms of the initial appointees should be staggered.

Third, considering the long delay in establishing the Board and the ACLU's assessment that there is an urgent need to reexamine the Privacy Act,[36] CPSR suggests that the Board's recommendations for amending the Privacy Act of 1974 be delivered to Congress one year from the date that the legislation takes effect.

Finally, the proposed legislation should address privacy issues for private sector record-keeping systems, particularly the secondary use of transactional data. Currently, there are widespread violations of Fair Information Practices; information which is not needed for a particular transaction is routinely obtained and used for unrelated purposes, or sold to other parties without the knowledge and consent of the consumer.

As privacy scholars have often noted, the United States, unlike most of Western Europe, has drawn a distinction between record systems operated by the government and those in the private sector. For this reason, argue some in industry, it would be inappropriate to regulate private sector privacy. However, this view ignores the record of privacy legislation in the United States during the last ten years. For if one lesson is clear, it is that Congress has shown itself willing to establish privacy safeguards in the private sector to ensure privacy protection, particularly where new technologies are involved.

For example, as the cable industry took off in the early 1980s concern about the privacy of subscribers information also grew. Congress responded. The Cable Communications Policy Act of 1984 prohibited a cable service from disclosing information about a subscriber's cable viewing habits without the individual's consent. The Act requires the cable service to inform the subscriber of the nature and use of personally identifiable information collected; the disclosures that may be made of such information; and the period during which such information will be maintained. The cable service must also provide subscribers access to information maintained about them.[37]

Electronic mail, a boon to communication, also raised concern about the security of the content of electronic messages. The Electronic Mail Association was as worried as its customers, perhaps more so, because of the concern that a new mail service would not be very useful if privacy could not be assured. The Electronic Communication Privacy Act of 1986 responded to the need for privacy protection for this new form of communication.[38]

And, when a nominee to the Supreme Court found that his choice of videos that he watched with his family in their home had become the subject of an article in a local newspaper, Congress enacted legislation to protect the rental list of video users.[39]

So, too, it should be with the sale of personal data, aggregated from separate lists, that are gathered and sold without adequate privacy safeguards or the knowledge and consent of the people involved. The Code of Fair Information Practices should be codified into law to provide this protection. The data protection principles of the Direct Marketing Association could also form the foundation for an enforceable legal right of information privacy.

The establishment of a data protection board is a modest first step that would shine some light on the privacy problems facing this country, and begin to propose solutions that could be adopted. This need not be an adversarial process that pits the Federal government against the private sector, but it must be a determined process, conducted with dedication and a commitment to individual liberty. This is also not about restricting technology; it is about the responsible application of technology so that risks to personal privacy are reduced.

There is a clear need to carry forward the principles embodied in privacy law in the United States and to ensure that Fair Information Practices apply to private sector record systems. The intimate details of our private lives enjoy the same protection whether big business or big government is the custodian. Absent clear privacy safeguards, we are left at the mercy of a rapidly evolving technology and an industry that can say little more than "trust us." This is at odds with the history of privacy protection in the United States and places the fragile freedom of American citizens in a precarious position.

ACKNOWLEDGMENTS

This article is adapted from prepared testimony on Computer Privacy and H.R. 3669, "The Data Protection Act of 1990," before the Subcommittee on Government Information, Justice and Agriculture, Committee on Government Operations, House of Representatives, May 16, 1990. The testimony was prepared with the assistance of Professor Mary J. Culnan, School of Business Administration, Georgetown University, and Dr. Ronni Rosenberg, Kennedy School of Government, Harvard University.

NOTES AND REFERENCES

1. The Association for Computing Machinery (ACM) Code of Professional Conduct states that:

   Ethical Considerations:

   EC5.1 An ACM member should consider the health, privacy, and general welfare of the public in the performance of his work.

   EC5.2 An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of individual privacy and seek the following:
   To minimize the data collected;
   To limit authorized access to the data;
   To provide proper security for the data;
   To determine the required retention period of the data;
   To ensure proper disposal of the data.

   The Data Processing Management Association (DPMA) Code of Ethics, Standards of Conduct and Enforcement Procedures states:

   "In Recognition of My Obligation to Society I Shall: Protect the privacy and confidentiality of all information entrusted to me"

   The preliminary code of ethics for the International Federation of Information Processing (IFIP) makes data protection a central provision of Individual Professional Ethics:

   1.2 Protection of Privacy

   Information Technology Professionals have a fundamental respect for the privacy and integrity of individuals, groups, and organizations. They are also aware that computerized invasion of privacy, without informed authorization and consent, is a major, continuing threat for potential abuse of individuals, groups, and populations. Public trust in informatics is contingent upon vigilant protection of established cultural and ethical norms of information privacy.

   Computers & Society, 36 (March 1990): 20 (Emphasis added).

2. Willis H. Ware, a noted computer scientist at the Rand Corporation, chaired the Secretary's Advisory Committee on Automated Personal Data Systems of the Department of Health, Education & Welfare. That Committee produced *Records, Computers and the Rights of Citizens* (1973), a landmark report which outlined the privacy risks of automated record systems, recommended various safeguards, and gave rise to the Privacy Act of 1974, the most comprehensive privacy law in the United States. Joseph Weizenbaum, an emeritus professor of Computer Science at MIT, was also a member of the Advisory Committee.

   Subsequent reports by the Office of Technology Assessment have often relied heavily on computer scientists to assess the privacy risks on automated information systems. See, e.g., *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Washington, DC: GPO, 1987).

3. See, e.g., Rein Turn, "Information Privacy Issues for the 1990s," "1990 *IEEE Symposium on Security and Privacy* 395.

4. See, e.g., Ronni Rosenberg, "Privacy in the Computer Age," *CPSR Newsletter*, 4 (1986–1987): 3–5; "FBI Fails to Allay Concern for Civil Liberties," *Government Computer News*, 19 (September 18, 1989) (letter from Marc Rotenberg, CPSR Washington Office Director) (FBI records system); "Phone Gadget Reveals Caller's Number," *The Los Angeles Times*, (December 1, 1989, p. D1 (caller ID); Marc Rotenberg, "The Only Locksmith in Town: The NSA's Efforts to Control the Dissemination of Cryptography," *Index on Censorship*, (January 1990), p. 12 (data communication privacy); Felicity Barringer, "Electronic Bulletin Boards Need Editing: No They Don't," *The New York Times*, (March 11, 1990), p. 6, section V (electronic speech); William Trombley, "Electronic Elections Seen as an Invitation to Fraud," *The Los Angeles Times*, (July 4, 1989), p. 1 (reliability of computerized vote counting).

   Most recently, CPSR sponsored a panel discussion at the Kennedy School of Government on the civil liberties implications of the use of expert systems by law enforcement agencies.

5. See *FBI Oversight and Authorization Request for Fiscal Year 1990: Hearings* before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, 101st Cong.,

1st Sess. (1989), pp. 512–596; Horning, Neumann, Redell, Godman & Gordon, *A Review of NCIC 2000 The Proposed Design for the National Crime Information Center* (1989) (Expert panel report), reprinted in Ibid., pp. 512–576.

6 "FBI Rejects Plans to Widen Computer's Data on Suspects," The *New York Times*, (March 4, 1989). "FBI Rejects Computer Use on Suspects: Plan Would Have Allowed Tracking Those Not Charged with a Crime," *The Washington Post*, (March 3, 1989), p. A6.

7 See, e.g., *Privacy and 1984: Public Opinions on Privacy Issues: Hearing* before a Subcommittee of the Committee on Government Operations, House of Representatives, 98th Cong., 1st Sess. (1984), pp. 9–75 (testimony of Lou Harris). See discussion infra, at 12.

8. David Linowes, the former chairman of the Privacy Protection Study Commission, detailed the efforts of Fortune 500 companies to protect the privacy interests of both customers and employees in *Privacy in America* (Champaign, IL: University of Illinois, 1989).

9. David Burnham, *The Rise of the Computer State* (New York: Random, 1983). See also Kenneth C. Laudon, *The Dossier Society* (New York: Columbia University Press, 1986); Linowes, *Privacy in America*, Robert Ellis Smith, Privacy (Washington, DC: Privacy Journal, 1980); Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967). Linowes found in his review of the recordkeeping practices of Fortune 500 companies that, not surprisingly, as discrete record systems within an organization were automated they were also brought together in consolidated databases (p. 60).

10. The problem of controlling the misuse of phone numbers has been directly addressed in Europe and is the subject of extended discussion in the United States.

11. H.W. William Caming, "Protection of Personal Data in the United States," *The Information Society*, 3 (1984): 118–122.

12. U.S. Department of Health, Education & Welfare, Records Computers and the Rights of Citizens (1973), p. 41.

13. A related goal is that organizations should seek to minimize the amount of personal information that is collected, since it is in the collection of information that unintended and unanticipated risks to privacy arise. "Data minimization" is a central theme of many privacy protection programs. See ACM Code, supra note 1; David Linowes, *Privacy in America* (1989), p. 175. For a discussion of the potential privacy risks in government information systems, absent an effort to reduce the collection of transactional data, see Marc Rotenberg, "The Computer Security of 1987 (P.L. 100-235) and the Memorandum of Understanding between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)," the Subcommittee on Legislation and National Security, Committee on Government Operations, House of Representatives, May 4, 1989 reprinted in *Military and Security Council of Computer Security Issues*, 101st Cong., 1st Sess. (1989), pp. 80, 106–108.

14. See, e.g., Lena H. Sun, "Giant to Test Supermarket Cash Rebates," *The Washington Post*, (June 14, 1989), p. A1; Michael Freitag, "In This Computer Age, Who Needs Coupons?," *The New York Times*, (June 15, 1989), p. 1; Lena H. Sun, "Checking out the Customer: New Technology Can Give Stores Detailed Knowledge about Buyer's Habits," *The Washington Post*, (July 9, 1989), p. H1; Mark Potts, "Giant to Widen 'Frequent Buyer' Rebate Test," The Washington Post, (September 16, 1989), p. D12; Martha Groves, "Frequent-Shopper Plans Are Wooing Customer," *The Los Angeles Times*, (October 1, 1989), p. 1. According to the Washington Post, customers who sign up for Reward America will receive cards with bar codes that will be scanned at Giant checkout counters. The data on the shoppers purchases will then be entered into a computer system. Customers will be sent monthly statement tallying their purchase of the roughly 100 products to be included in the program. When they satisfy a specific purchase requirement, they will receive rebate vouchers that can be redeemed at Giant stores.

15. These data collection practices could be described as misleading at best. For example, one of the conditions specified in the application for Safeway's Preferred Customer Program is that customers "agree to allow Safeway Stores, Incorporated and their processing supplier to record and make use of information about products they purchase." It is hard to believe that by signing this agreement customers have given Citicorp permission to sell detailed information about themselves and their purchase to unspecified third parties.

16. "Retail New Outlet for Lists on CD-ROM," *Direct Marketing*, (May 1990), p. 10.

17. "Corporate Stars of the Future," *The Wall Street Journal*, (July 8, 1990), p. A30. Another major information vendor, TRW, already offers a locator service called Sherlock that scans through computer data to determine the most recent address of individuals.

18. "New Service Offers Marketing Data on 120 Million People," *The Privacy Times*, (May 9, 1990), pp. 1, 2.

19. Mary J. Culnan, "Bill of Rights? Or Bill of Goods," *The New York Times*, (January 21, 1990), p. E21 (op-ed).
20. Mary Lu Carnevale, "Phone Data Enters the Junk-Mail Morass," *The Wall Street Journal*, (May 4, 1990), p. A5A.
21. *Direct Marketing*, May 1990.
22. "Using Medical Information for Marketing," *Privacy Journal*, 16 (February 1990): 1.
23. American Express Survey (1986). Another recent survey shows similar concern for privacy protection and support for new privacy legislation. According to *Cambridge Reports Trends & Forecasts* (May 1989, p. 6), seven out of ten people say that personal privacy is very important; three-quarters of the population are concerned that their privacy is actually threatened; and the majority of those expressing an opinion believe that Federal privacy laws should be strengthened. Professor Alan Westin is expected to release a new privacy survey later this year.
24. Jo Anne Parker, "The Real Privacy Issues," *Target Marketing Magazine*, (November 1988), p. 6, quoted in Mary Gardiner Jones, "Privacy: Significant Marketing Issues for the 1990s," p. 13 (Available from Consumer Interest Research Institute, Washington, DC).
25. *Cambridge Reports Trends and Forecasts*, (May 1989), p. 6.
26. *The Computer and the Invasion of Privacy*, Hearings before the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, House of Representatives, 89th Cong., 2d Sess. (1966), p. 6.
27. *Hearings on Federal Data Banks, Computers, and the Bill of Rights* before the subcommittee on Constitutional Rights of the Senate Judiciary Committee, 92nd Cong., 1st Sess., p. 761, as quoted in Records, Computer and the Rights of Citizens (1973), p. 225.
28. See Linowes' *Privacy in America*.
29. "Rollout: on Privacy," *Direct Marketing*, (May 1989), p. 4 (noted with approval by Raymond Roel, the Editor).
30. See Albinger, "Personal Information in Government Agency Records: Toward an Informational Right to Privacy," *Annual Survey of American Law* (1986), pp. 625, 642 n. 150.
31. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, Report of the Commission (Washington, DC: GPO, 1977), p. 37.
32. David H. Flaherty, *Protecting Privacy Protection in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill, NC: University of North Carolina Press, 1989), p. 304.
33. See George Trubow, *Watching the Watchers: The Coordination of Federal Privacy Policy* (Washington, DC: Benton Foundation Project on Communications & Information Policy Options, n.d.), pp. 9–10; Albinger, supra note 26, pp. 642–643.
34. The need for the development of data protection policies in the United States was made clear at a recent meeting in Luxembourg with the European Council and the Council of Europe on access to public information, data protection and computer fraud. Participants were told that countries that do not develop data protection laws by 1992 may face curtailment of transborder data flow. Thus far, seven of the twelve member countries of the European community have developed data protection laws. See *Access Reports*, 16 (April 4, 1990): 6–10 (report of Tom Riley).

    Greater participation by the United States in the deliberation of European data protection law could improve privacy protection in this country. For example, the Council of Europe convention on data protection provides a good model for data protection standards:

    Personal data to be automatically processed shall be: (1) obtained and processed fairly and lawfully, (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes, (c) adequate, relevant, and not excessive for the purpose for which they are maintained, (d) accurate, and where necessary, kept up to date, and (e) preserved in form which permits identification of the data subjects for no longer than required for the purposes for which those data are kept.

    Convention on Protection of Individuals with Regard to Automatic Processing of Personal Data, The Council of Europe, Strassbourg, France, January 28, 1981, quoted in Rein Turn, "Information Privacy Issues for the 1990s," *IEEE Symposium on Security and Privacy* (1990), p. 397.
35. Supra note 9.
36. Jerry Berman and Janlori Goldman, *A Federal Right of Information Privacy: The Need for Reform* (Washington, DC, Benton Foundation Project on Communications & Information Policy Options, n.d.).

37 P.L. 98-549.

38 P.L. 99-508. ECPA amends the Federal wiretap statue to prohibit the unauthorized interception and disclosure of electronic communications made possible by new technologies, such as cellular phones, electronic mail, and satellite television transmissions. The law defines electronic communications, restricts disclosure of stored communications, and creates civil and criminal penalties for individuals who, without authorization, willfully intercept or disclose the contents of electronic communications or who access such communications while in electronic storage. 18 U.S.C. 2510 et seq. (West 1989).

39 P.L. 100-618. Representative Al McCandless introduced the first video privacy bill in the 100th Congress, and subsequently testified in support of the bill that became the Video Privacy Protection Act. See The Video Privacy Protection Act of 1988, S. Rep. No. 599, 100th Cong., 2nd Sess. (1989), (testimony of Representative McCandless).