PROTECTING PRIVACY AND PREVENTING THE MISUSE OF SOCIAL SECURITY NUMBERS

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MAY 22, 2001

Serial No. 107–31

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

74–226 WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

PHILIP M. CRANE, Illinois
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHIL ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY C. HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas
EARL POMEROY, North Dakota

ALLISON GILES, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

E. CLAY SHAW, JR. Florida, *Chairman*

SAM JOHNSON, Texas
MAC COLLINS, Georgia
J.D. HAYWORTH, Arizona
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

ROBERT T. MATSUI, California
LLOYD DOGGETT, Texas
BENJAMIN L. CARDIN, Maryland
EARL POMEROY, North Dakota
XAVIER BECERRA, California

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

	Page
Advisory of May 15, 2001, announcing the hearing	2

WITNESSES

Social Security Administration:	
Hon. James G. Huse, Jr., Inspector General, Office of the Inspector General	16
Michael Robinson, Special Agent, Office of the Inspector General	19

Electronic Privacy Information Center, and Georgetown University Law Center, Marc Rotenberg	102
Financial Services Coordinating Council, and Covington & Burling, John C. Dugan	92
Individual Reference Services Group, and Piper Marbury Rudnick & Wolfe LLP, Ronald L. Plesser	109
Kravit, Cory B., University of Florida	80
Moneme, Emeka, Washington, DC	13
New York City Police Department, Michael Fabozzi, accompanied by James Doyle	59
Pension Benefit Information, Paula LeRoy	113
Privacy Times, Evan Hendricks	85
Robinson, Nicole, Oxon Hill, MD	9
Texas, Harris County, Charles Bacarisse	77
U.S. Public Interest Research Group, Edmund Mierzwinski	116

SUBMISSIONS FOR THE RECORD

Conference of State Court Administrators, Arlington, VA, David K. Byers, statement	148
National Conference of State Legislatures, Hon. Brian Flaherty, letter	151
National Council of Investigation and Security Services, Inc., Bruce Hulme, statement	153
National Council on Teacher Retirement, Arlington, VA, Cynthia L. Moore, statement	157
Paul, Hon. Ron, a Representative in Congress from the State of Texas, statement	158

PROTECTING PRIVACY AND PREVENTING THE MISUSE OF SOCIAL SECURITY NUMBERS

TUESDAY, MAY 22, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:05 a.m., in room 1100 Longworth House Office Building, Hon. E. Clay Shaw, Jr. (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
May 15, 2001
No. SS–4

Contact: (202) 225–9263

Shaw Announces Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers

Congressman E. Clay Shaw, Jr., (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on protecting the privacy and preventing misuse of Social Security numbers (SSNs). **The hearing will take place on Tuesday, May 22, 2001, in room B–318 Rayburn House Office Building, beginning at 10:00 a.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. Witnesses will include the Social Security Administration's (SSA's) Office of the Inspector General, victims of SSN misuse and representatives from consumer groups, businesses, and State and local government. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

SSNs were created in 1936 for the sole purpose of tracking workers' Social Security earnings, but today the SSN is commonly used as a personal identifier. SSNs are required by law for the administration of several Federal programs, such as the income tax, the Food Stamp program, and Medicaid. SSNs are also commonly used in the private sector, as many businesses require individuals to disclose their SSN as a condition for doing business. In fact, according to the SSA, the SSN is the single-most widely used record identifier in the public and private sectors.

The exploding use of SSNs has intensified the public debate over the use and misuse of SSNs in today's society. Some believe that the expanded use of the SSN benefits the public by improving access to financial and credit services in a timely manner, reducing administrative costs, and improving record-keeping so consumers can be contacted and identified accurately, thus reducing the chance of "identity theft." Others argue that the pervasive use of SSNs, and the seemingly ease by which another person's SSN may be obtained, makes SSNs a primary target for fraud and misuse. In 1999, of the 75,000 fraud allegations received by SSA's Office of Inspector General fraud hotline, over 80 percent involved misuse of the SSN. In addition to concerns about SSN misuse, privacy concerns have been raised as companies increasingly share and sell personal information without the customer's knowledge or consent.

Primarily, there are three laws aimed at protecting privacy and reducing SSN misuse. The "Privacy Act of 1974" (P.L. 93–579) prohibits Federal agencies from disclosing personal information including the SSN, without the individual's consent. The "Identity Theft and Assumption Deterrence Act of 1998," (P.L. 105–318) makes it a Federal crime to assume another person's means of identification. The "Gramm-Leach-Bliley Act," (P.L. 106–102) enacted in 1999, includes provisions requiring financial institutions to protect the privacy of the personal financial information of their customers. However, no Federal law regulates the overall use of SSNs and Federal laws neither require nor prohibit other public and private uses of the SSN.

In recent years, several legislative proposals aimed at protecting consumer privacy and curbing fraudulent use of SSNs have been introduced.

During the 106th Congress, two hearings were held by the Subcommittee examining the use and misuse of SSNs. As a result, H.R. 4857, the "Social Security Number Privacy and Identity Theft Prevention Act of 2000," was introduced on a bipartisan basis by Subcommittee Chairman Shaw, Ranking Member Robert T. Matsui (D–CA), along with Rep. Gerald D. Kleczka (D–WI) and other Members of the Committee on Ways and Means. The bill included provisions to prohibit the sale and display of the SSN by Federal, State and local governments, increase fines and penalties for SSN misuse, and prohibit the sale of SSN's by the private sector. While H.R. 4857 was approved by the Committee on Ways and Means at the end of last year, it was not considered by the full House of Representatives before the end of the session, due to its referral to other Committees of jurisdiction who did not take action on the bill.

In announcing the hearing, Chairman Shaw stated: "Social Security numbers were developed to ensure Americans' hard-earned wages were properly credited to their Social Security records. Although SSNs were never intended to be a personal identifier, their use is pervasive throughout today's mobile, automated society. Many would argue the use of SSNs makes sense in certain Federal programs, where it is required and protected by law—such as Medicare and Food Stamps or to determine one's credit worthiness. However, today more and more people are being told their SSN is required for reasons that just don't make sense, like renting a video, making funeral arrangements for a loved one, or even picking up Girl Scout cookies. Our challenge is to find ways to make sure SSNs are used only when absolutely necessary and that once shared, SSNs remain private and are only used for the purpose for which they were requested in the first place."

FOCUS OF THE HEARING:

The hearing will focus on the widespread use and misuse of the SSN in the public and private sectors. In addition, the Subcommittee will examine legislative proposals aimed at combating SSN misuse and protecting privacy, including the impact of such proposals on businesses, governments, and consumers.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should *submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, with their name, address, and hearing date noted on a label,* by the *close of business,* Tuesday, June 5, 2001, to Allison Giles, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Subcommittee on Social Security office, room B–316 Rayburn House Office Building, by close of business the day before the hearing.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be submitted on an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, typed in single space and may not exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers where the witness or the designated representative may be reached. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press, and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at "http://waysandmeans.house.gov".

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman SHAW. Good morning. Today we continue our quest to protect the privacy of every American by cracking down on the fraud, abuse and theft of Social Security numbers or perhaps I should say the availability of the Social Security numbers (SSN) to commit fraud, abuse and theft.

Last year, as learned from Colonel and Mrs. Stevens of Maryland, identity theft is truly a devastating crime. Their Social Security numbers used on 33 fraudulent accounts and $113,000 of bad debt—that is the problem that Colonel and Mrs. Stevens had. And Mr. Bob Horowitz, who is a single father in my congressional district, saw his number used to open five fraudulent credit accounts. Months and years later they were still spending time, money and energy to clear their names. No wonder in a Wall Street Journal poll just last year respondents ranked privacy as their number one concern in the 21st century, ahead of wars, terrorism and environmental disasters.

When Social Security numbers were created 65 years ago their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today use of the Social Security number is rampant. We have literally developed a culture of dependence on Social Security numbers. Businesses and governments use of the number as a primary way of identifying individuals. All of us know difficult it is to conduct even the most frivolous transaction without having to cough up our Social Security number first.

Although Social Security numbers are used for many legitimate purposes, the wide availability and easy access to this very personal information has greatly facilitated Social Security number-related crimes and has generated a growing concern for our own privacy.

Clearly, there is a need for a comprehensive law that will better protect the privacy of Social Security numbers and protect the American public from being victimized. Last year I, along with Mr. Matsui, Mr. Kleczka and Mr. Foley and other Subcommittee mem-

bers, introduced H.R. 4857, the Social Security Number Privacy and Identity Theft Protection Act of 2000. This legislation took a comprehensive approach to achieve this goal by targeting the treatment of Social Security numbers in both the public and the private sectors.

In the public sector, the bill restricted the sale and public display of Social Security numbers, provided for enforcement of the provisions and established penalties for the violation. In the private sector, the bill restricted the sale, purchase and display of Social Security numbers, limited the dissemination of the Social Security numbers by credit-reporting agencies, and made it more difficult for businesses to deny services if a customer refused to provide his or her Social Security number.

While H.R. 4857 was approved by the Committee on Ways and Means at the end of last year, it was not considered by the full House before the end of the session due to its referral to other committees of jurisdiction, which did not take action on the bill—the Judiciary Committee, which waived jurisdiction, and the Commerce Committee, which did not have time to hold hearings and to act on the bill.

In our hearing today, we will hear from two more of the countless numbers of victims who have had their identities stolen—Miss Nicole Robinson and Emeka Moneme. We will then hear from law enforcement officials who will discuss the challenges they face as they try to catch these identity thieves. Finally, we will hear from representatives from the business groups, elected officials and privacy advocates who will share with us their impressions on the widespread use and misuse of Social Security numbers in the public and private sectors, as well as their views on the impact of legislative proposals.

One of these witnesses, I might add, was an intern in my office when we were working on this issue and went down and worked to eliminate the use of these numbers at the University of Florida.

This week I, along with several of my Ways and Means Committee, plan to reintroduce our bipartisan legislation. I will then work with my colleagues on the Ways and Means Committee and from the other committees of jurisdiction to quickly bring to the House floor comprehensive legislation to keep Social Security numbers private and protect citizens from identity theft. The time for action is long overdue and I am hopeful that the other committees will follow suit and have hearings on this legislation.

Mr. Becerra.

[The opening statement of Chairman Shaw follows:]

Opening Statement of the Hon. E. Clay Shaw, Jr., a Representative in Congress from the State of Florida, and Chairman, Subcommittee on Social Security

Today we continue our quest to protect the privacy of every American by cracking down on the fraud, abuse, and theft of Social Security numbers (SSNs).

Last year, as we learned from Colonel and Mrs. Stevens of Maryland, identity theft is a truly devastating crime. Their Social Security numbers used on 33 fraudulent accounts and $113,000 of bad debt. And Mr. Bob Horowitz, a single father and small business owner from my district, saw his number used to open five fraudulent credit accounts. Months and years later, they were still spending time, money, and energy to clear their names.

No wonder in a Wall St. Journal poll last year, respondents ranked privacy as their number one concern in the 21st century, ahead of wars, terrorism, and environmental disasters.

When Social Security numbers were created 65 years ago, their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today, use of the Social Security number is rampant.

We have literally developed a culture of dependence on the Social Security number. Businesses and governments use the number as the primary way of identifying individuals. All of us know how difficult it is to conduct even the most frivolous transactions without having to cough up our Social Security numbers first.

Although Social Security numbers are used for many legitimate purposes, the wide availability and easy access to this very personal information has greatly facilitated Social Security number-related crimes and generated a growing concern of privacy. Clearly, there is a need for a comprehensive law that will better protect the privacy of Social Security numbers and protect the American public from being victimized.

Last year, I along with Mr. Matsui, Mr. Kleczka, Mr. Foley, and other Subcommittee members introduced H.R. 4857—the Social Security Number Privacy and Identity Theft Prevention Act of 2000. This legislation took a comprehensive approach to achieve this goal by targeting the treatment of Social Security numbers in both the public and private sectors.

In the public sector, the bill restricted the sale and public display of Social Security numbers, provided for enforcement of the provisions, and established penalties for violations.

In the private sector, the bill restricted the sale, purchase, and display of Social Security numbers, limited dissemination of the Social Security number by credit reporting agencies, and made it more difficult for businesses to deny services if a customer refused to provide his or her Social Security number.

While H.R. 4857 was approved by the Committee on Ways and Means at the end of last year, it was not considered by the full House of Representatives before the end of the session, due to its referral to other Committees of jurisdiction who did not take action on the bill.

In our hearing today, we will hear from two more of the countless number of victims who have had their identity stolen, Nicole Robinson and Emeka Moneme (Emecca Moan-a-may).

We will then hear from law enforcement officials who will discuss the challenges they face as they try to catch these identity thieves.

Finally we will hear from representatives from business groups, elected officials, and privacy advocates who will share with us their impressions on the widespread use and misuse of the SSN in the public and private sectors as well as their views on the impact of legislative proposals.

This week, I, along with several of my Ways and Means colleagues, plan to reintroduce our bipartisan legislation. I will then work with my colleagues from Ways and Means, and from the other Committees of jurisdiction, to quickly bring to the House floor comprehensive legislation to keep Social Security numbers private and protect citizens from identity theft. The time for action is long overdue.

Mr. BECERRA. Thank you, Mr. Chairman. Let me just say that on behalf of ranking member Matsui and the members of the Committee, we are pleased to have this hearing hosted today, as well, given that this is a bipartisan piece of legislation that has worked its way through the House in the past and we are looking forward to working with you, Mr. Chairman, to try to see if we cannot get something done.

I do not think there is anyone here who would not recognize that we do have a problem with regard to the Social Security number. We know that it was a number that was initially created for the purposes only of the Social Security Administration to track those who were to receive benefits through the Social Security Administration. Now, or course, we use it day to day in all of our lives and we find now that the statistics associated with identity theft are

staggering. There is no doubt that if we do not do something, we are going to continue to see the numbers just increase.

I understand that from the Federal Trade Commission (FTC) with its theft hotline that they are receiving somewhere on the average of 1,000 calls per week, some 60 percent of which relate to actually identity theft from people who are calling as victims of that identity theft. We know that the numbers in terms of dollars are staggering. Anywhere from $250 in losses to up to $200,000 in losses have been reported by individuals.

But, we also know that the number can be used for good purposes, as well. The contributions that the use of the Social Security number makes to program administration and to business efficiency are certainly there and we have to be cognizant of that. Certainly, though, we have to be mindful and very careful that we do not allow some of our most fundamental rights—the right to privacy and the right to control our personal information—be abridged in the name of expediency, however.

So, Mr. Chairman, I believe we are very much looking forward to hearing from the witnesses, to trying to move this bipartisan piece of legislation forward and, at the end, hopefully providing people in this country with a greater sense of security that their Social Security number will go for a good purpose, in helping them obtain their Social Security benefits in the future but, most importantly, to make sure that day to day, that Social Security number will be protected.

Thank you, Mr. Chairman.

Chairman SHAW. Thank you.

Mr. Kleczka, did you want to make a couple of comments? I know this is unusual at a hearing, to have two members make opening comments, particularly from the minority side, but I would be delighted to yield to you if you have any comments.

Mr. KLECZKA. Thank you, Mr. Chairman. The only thing I would like to say is thank you to all the witnesses who are here to tell their stories. There are countless others who are not here today who have also been victims of identity theft.

I think it is high time that Congress recognize that the Social Security number is not a national identifier and for businesses who, by habit or for other reasons, request our numbers—I recall a few years ago when I was checking out at Toys R Us. The items were for my nieces and nephews, not for me. The clerk demanded my Social Security number on my check. Well, that seemed kind of odd but I think the person was told to ask for that so I wrote down any 10 numbers that came to mind, gave her the check and she processed the payment. But if I were her or any clerk I would like to see a person's driver's license number versus a Social Security number because that does not tell anything.

So, I just received a copy of the Congress Daily today where the retailers are indicating this is a knee-jerk reaction on the part of Congress. To the 750,000 Americans who are going to be victims of identity fraud this year, I do not think that is knee-jerk. And we are going to hear from witnesses where they are going to say that it takes years to clear your own record because the knee-jerk reaction from the credit bureaus is "Yeah, we hear that all the time; that is not your charge." So you have to go back and, through var-

ious means, prove that you did not make those changes and then finally, clear your own records so that you can get additional credit or whatever.

So, Mr. Chairman, I am honored not only to be at the Committee hearing this morning but also to cosponsor the bill and hopefully we have enough time this session that we will see enactment of this much-needed legislation. Thank you very much.

[The opening statement of Mr. Kleczka follows:]

Opening Statement of the Hon. Gerald D. Kleczka, a Representative in Congress from the State of Wisconsin

I would like to thank the Chairman for holding this hearing at continuing his efforts on this very important issue. In addition, I would like to congratulate Mr. Shaw for working in a bipartisan way with Ranking Member Matsui and myself. The success of last year's Social Security Number Privacy and Identity Theft Prevention Act, which was passed by the full Committee, demonstrates the support for legislation to protect our personal information.

We take for granted that our personal information is private. Unfortunately, that's not the case. We must take action to guard access to our personal information because it's not a commodity to be bought or sold. We as consumers should have the final say over how that information can be used, not some marketing firm.

Social Security numbers have become our default identifiers for many businesses, and thereby the key to much of our most personal information. That has to stop. As identity theft and fraud increases, action must be taken to ensure that this personal information remains private.

My colleagues know that their constituents are quickly becoming aware of how little privacy they have. In fact, since I introduced my first bill on this subject back in the 104th Congress, the debate has shifted from if we should pass legislation to protect personal information privacy to what type of legislation should be passed.

Fortunately, privacy advocates in Congress are beginning to have some success. For example, our colleague in the Senate, Mr. Shelby of Alabama, included language in the FY 2000 Transportation Appropriations bill defining in law, for the first time, SSNs as "highly personal information." This is a great start, but there's a lot more to be done. We must curb the rampant use of SSNs as personal identifiers. This hearing is an important step toward developing more complete personal privacy protection.

To that end, I have introduced legislation, the Personal Information Privacy Act (PIPA)—H.R. 1478, that safeguards consumers' personal privacy by giving them the ability to protect their personal information from being bought and sold by third parties.

This bill would restore consumer control over personal information by requiring that a third party obtain consent from an individual before making commercial use of that person's Social Security number (SSN). In fact, any non-criminal use not explicitly allowed by law would face this restriction, including the growing commercial use of SSNs as personal identifiers by various businesses.

Under my legislation, refusing to sell services or goods to consumers who choose not to furnish their SSN would be illegal under the Federal Trade Commission Act, and businesses would be liable for up to $10,000 in fines per violation for committing unfair or deceptive business practices. Credit bureaus would also be prevented from giving out SSNs without a person's consent. My bill would amend the Fair Credit Reporting Act and the Social Security Act to authorize civil penalties for privacy violations ranging from $25,000 to $500,000.

Information on products or services bought by an individual and from where they were purchased—also known as transaction histories—could not be sold or transferred for marketing purposes unless a consumer gives written consent.

Hopefully Congress will enact H.R. 1478. In the meantime, I look forward to working with Chairman Shaw on passing legislation that will protect the privacy of our personal information.

Chairman SHAW. Thank you.

Our first panel of witnesses is made up of—we will start out with two victims. Nicole Robinson from Oxon Hill, Maryland. Emeka

Moneme, who is from Washington, DC, an employee of the Washington, DC government. The Honorable James G. Huse, who is the Inspector General, the Office of the Inspector General, Social Security Administration. Mike Robinson, who is a special agent, the Office of the Inspector General, the Social Security Administration. Michael Fabozzi, who is a detective, Computer Investigations and Technology Unit of the New York City Police Department and he is accompanied by James Doyle, who is a sergeant, Computer Investigations and Technology Unit of the New York City Police Department.

All the witnesses, we welcome you. Your complete statements will be put into the record and we invite you to summarize as you may be comfortable, and we will start with you, Miss Robinson.

STATEMENT OF NICOLE ROBINSON, OXON HILL, MARYLAND

Ms. ROBINSON. Good morning, Mr. Chairman, distinguished members of the Committee. My name is Nicole Robinson and I am a victim of ID theft.

One Friday evening in early April 2000 I was contacted by a fraud investigator of a national jewelry chain. He informed me that an individual had opened an instant credit account for $3,200 and bought two watches and a ring in a mall in San Antonio a day before. He asked me if I was Nicole Robinson, he confirmed my date of birth, my Maryland address, and told me what Social Security number was provided on the credit application. My stomach turned when he recited mine.

The criminal had returned that day and attempted to purchase more merchandise, which the salesperson thought was suspicious. The salespeople told her that their computers were down and then alerted their fraud department and the San Antonio police.

A thousand thoughts raced through my mind that weekend. How could this have happened to me? Was it a friend of mine, an acquaintance, an enemy? How many accounts had been opened?

On Monday I contacted the three credit-reporting agencies to see if there were any accounts that were opened recently and there were no new accounts, yet. There were a lot of inquiries. One of the inquiries was from my mortgage lender. I contacted them and alerted them to the fact that there was a woman in Texas using my identity to obtain credit. They confirmed that a woman had provided my information in connection with an application for a personal loan in the amount of $1,800. At my suggestion, a few days later they contacted her to tell her she was approved for the loan. She was arrested by the San Antonio police when she left the office with the check.

After she was arrested they asked her where she obtained my Social Security number and date of birth. She told them that she worked for a business that maintained Health Maintenance Organization (HMO) databases. She searched that information to get my Social Security number and date of birth.

She was charged with making a false statement to obtain goods. She was released a few days later after she, her pastor and parents, assured a Bexar County judge that she would not do this again. Two days later she applied for a mortgage in my name.

When I finally received my credit reports in the mail there were several changes. I saw that she had made up middle names for my middle name, since she did not know what my middle name was. She had provided a fictitious maiden name, several different addresses in Texas and several different dates of birth, but she always provided my Social Security number. On one application she provided my Social Security number with the last two numbers transposed and a bogus Texas address and she was still approved for the items she sought. When the bills for the item were returned from the fake address, the creditor reviewed my credit report again and sent several of her delinquent bills to my home in Maryland. When I contacted them by phone they were rude and did not want to believe that the account was fraudulent and then refused to send me an affidavit of fraud. Shortly after I contacted them they located the woman in San Antonio and repossessed the item from a warehouse. Now, a year later, they still have not acknowledged the account as fraudulent but I no longer receive her bills.

In the ensuing months I would discover that she also applied and was approved for two computers, large appliances, clothing, household goods, a cellular phone and a $1,600 vacuum cleaner. Some items were obtained even after fraud alerts were placed on my credit reports.

In June of 2000, two months after her arrest, she shopped for a car with my identity. She eventually purchased a 2000 Mitsubishi automobile from a San Antonio dealership. Although it took me until January 2001 to verify that the car was not purchased using my identity, GEICO insured the car for her in June of 2000 using my identity. When I contacted GEICO last June to obtain the VIN number of the vehicle, they refused to give it to me, citing their policy on protecting the privacy of their policyholders. I thought that was ironic since technically the policy that they issued was to me. She was able to obtain $36,000 worth of goods in a three-month period.

This has impacted my life greatly. I received delinquent bills for purchases she had made. I spent countless hours on calls to creditors in Texas who were reluctant to believe that the accounts that had been opened were fraudulent. I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and to have her charged with theft of my identity. She was never charged with identity theft and I had to pay for the collect call just to file the police report in Texas.

I tried to contact the district attorney's office in Bexar County to see what I could do to have her charged and no one ever responded to my messages. I had to send more than 50 letters to creditors trying to have them remove the more than 60 inquires that were made by this woman between March and June of 2000.

Just when I was starting to believe that this was over, I received a collection notice in her name at my home in Maryland on April 4 of this year. When I contacted the collection agency to tell them that they had the wrong person, I was told that the Social Security number that was provided for the loan was not mine. The gentleman at the collection agency told me that they had a bad address in San Antonio so information was given to their research department and they came up with my address in Maryland. I asked

him what service was connecting my address with this woman, who was committing felonies in Texas and he would not provide that information. I have since contacted him three times and he still has not returned my calls. I still do not know how they connected me with this woman and it concerns me since she has assumed several identities of persons named Nicole Robinson in order to commit fraud.

This crime has impacted my ability to refinance my home, obtain a line of credit at my bank, get cellular phone service. It has even affected accounts that I had prior to the crime. I subsequently had two lines of credit, both with zero balances and in good standing, closed because the businesses suspected that they, too, were fraudulent. I was told that I would have to reapply if I wanted the accounts reopened. Most importantly, this crime continues to give me constant anxiety.

I had always been a person who kept my Social Security card under lock and key. I never gave personal information over the phone and I always shredded and systematically discarded pre-approved credit applications. And I check my credit reports every year. I was not a likely victim. But since HMOs require my Social Security number and use it as an identification number, I was forced to be a victim.

Our government-issued Social Security numbers are being used daily. We provide our Social Security numbers to businesses on a regular basis for no reason other than their own internal use. I had no control over how mine was used or who had access to it. And until this happened to me I honestly did not give it much thought.

Since I have become a victim, I think about it every day. This will impact my life forever. Detective Victor Flores of the San Antonio Police Department told me, "There is nothing you can do and when she gets out of jail on the theft charges she will do it again. The recidivism rate is very high." When I tried to contact the detective to find out what happened to this woman he did not return my calls.

Chairman SHAW. Thank you, Miss Robinson. If you will supply me with the name and address of the people who would not return your calls I will see that they get a copy of your testimony and a letter from me telling them of this particular hearing.

Ms. ROBINSON. Thank you.

[The prepared statement of Ms. Robinson follows:]

Statement of Nicole Robinson, Oxon Hill, Maryland

I am a victim of ID theft. One Friday evening in early April 2000, I was contacted by a fraud investigator of a national jewelry chain. He informed me that an individual had opened an instant credit account for $3,200.00 and bought two watches and a ring in a mall in San Antonio a day before. He asked me if I was Nicole Robinson, he confirmed my date of birth, my Maryland address, and told me what social security number was provided on the credit application—my stomach turned when he recited mine. The criminal had returned that day and attempted to purchase more merchandise—which the sales person thought was suspicious. The sales people told her that their computers were down and then alerted their fraud department and the San Antonio police. A thousand thoughts raced through my mind that weekend. How this could have happened? Was it a friend of mine, an acquaintance, an enemy? How many accounts had been opened?

On Monday I contacted the three credit reporting agencies to see if there were any accounts that were opened recently and there were no new accounts on my reports—yet. There were a lot of inquiries. One of the inquiries was from my mortgage

lender. I contacted them and alerted them to the fact that there was a woman in Texas using my identity to obtain credit. They confirmed that a woman had provided my information in connection with an application for a personal loan in the amount of $1800.00. At my suggestion, a few days later they contacted her to tell her she was approved for the loan. She was arrested by the San Antonio police when she left the office with the check. After she was arrested, they asked her where she obtained my social security number and date of birth. She told them that she worked for a business that maintained HMO databases. She searched that information to get my social security number and date of birth. She was charged with "making a false statement to obtain goods". She was released a few days later after she, her pastor, and parents assured a judge that she would not do this again. Two days after her release, she applied for a mortgage.

When I finally received my credit reports in the mail, there were several changes. I saw that she had made up middle names for my middle initial since she did not know my middle name. She had provided a fictitious maiden name, several different addresses in Texas and several different dates of birth but she always provided my social security number. On one application she provided my social security number with the last two numbers transposed, and a bogus Texas address and she was still approved for the item she sought. When the bills for the item were returned from the fake address the creditor reviewed my credit report again and sent several of her delinquent bills to my home in Maryland. When I contacted them by phone, they were rude and did not want to believe the account was fraudulent then refused to send me an affidavit of fraud. Shortly after I contacted them, they located the woman in San Antonio and repossessed the item from a warehouse. Now, a year later they have still not acknowledged the account as fraudulent but I no longer receive bills.

In the ensuing months I would discover that she also applied and was approved for two computers, large appliances, clothing, household goods, a cellular phone and a $1600.00 vacuum cleaner. Some items were obtained even after fraud alerts had been placed on my credit reports. In June of 2000, two months after her arrest, she shopped for a car with my identity. She eventually purchased a 2000 Mitsubishi automobile from a San Antonio dealership. Although it took me until January 2001 to verify that the car was not purchased using my identity, Geico insured the car in June 2000 using my identity. When I contacted Geico in June to obtain the VIN number of the vehicle they refused to give it to me citing their policy on protecting the privacy of their policy holders. I thought that was ironic, since technically the policy they issued was to me. She was able to obtain $36,000.00 worth of goods in a three month period.

This has impacted my life greatly. I received delinquent bills for purchases she had made. I spent countless hours on calls with creditors in Texas who were reluctant to believe that the accounts that had been opened were fraudulent. I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and to have her charged with theft of my identity. She was never charged with identity theft and I had to pay for the collect call to file the police report. I tried to contact the district attorney's office to see what I could do to have her charged and no one ever responded to my messages. I had to send more than fifty letters to creditors trying to have them remove the more than 60 inquires that were made by this woman between March and June of 2000.

When I was starting to believe that this was over, I received a collection notice in her name at my home in Maryland on April 4 of this year. When I contacted the collection agency to tell them that they had the wrong person, I was told that the social security number that I provided for the loan was not mine. The gentleman at the collection agency told me that they had a bad address in San Antonio so information was given to their research department and they came up with my address in Maryland. I asked him what service was connecting my address with this woman who was committing felonies in Texas and he would not provide that information. I have since contacted him three times and he still has not returned my calls. I still don't know how they connected me with this woman and it concerns me since she has assumed several identities of persons named Nicole Robinson in order to commit fraud.

This crime has impacted my ability to refinance my home, obtain a line of credit at my bank, get cellular phone service. It has even affected accounts that I had prior to the crime. I subsequently had two lines of credit, both with zero balances and in good standing, closed because the businesses suspected that they too were fraudulent. I was told that I would have to reapply if I wanted the accounts re-opened. Most importantly this crime continues to give me constant anxiety.

I had always been a person who kept my social security card under lock and key, I never gave personal information over the phone, I always shredded and systemati-

cally discarded pre-approved credit applications and I checked my credit reports every year. I was not a likely victim—but since HMOs "required" my social and used it as an identification number—I was forced to be a victim. Our government issued social security numbers are being used daily. We provide our social security numbers to businesses on a regular basis for no reason other than their own internal use. I had no control over how mine was used or who had access to it—and until this happened to me, I honestly did not give it much thought. Since I have become a victim, I think about it every day. This will impact my life forever. Detective Victor Flores in San Antonio told me, "There is nothing you can do, and when she gets out of jail on the theft charge, she'll do it again. The recidivism rate is very high." When I tried to contact the detective to find out what happened to this woman, he didn't return my calls.

ID Victim

Someone stole my identity
I now feel I am no longer me
I reside in the pocket of a felon who can see
That she is allowed to steal me without penalty
She carries me casually, and each time she pulls me out
A small piece of me falls away—which leaves me no doubt
That someday soon I will enter a place
And the person I once knew as me will be wearing a felon's face
—Nicole Robinson

Nicole Robinson is a Maryland resident and an Information Technician for a government contractor.

Chairman SHAW. Mr. Moneme.

STATEMENT OF EMEKA MONEME, WASHINGTON, DC

Mr. MONEME. Mr. Chairman and distinguished members of the Subcommittee, good morning. My name is Emeka Moneme and I would first like to thank the Subcommittee for the invitation to share my personal experience dealing with identity fraud and specifically the misuse of my Social Security number. I hope to convey to you, as Miss Robinson just did, the frustration, anger and violation that comes as a part of this crime. But as I am sure other victims can attest, it is very difficult to actually express or even to comprehend it unless you have been a victim.

When I try to pull together the circumstances that surround the misuse of my information, it appears that the only piece of information that the perpetrator of this crime had to use was my Social Security number. My personal property was stolen at the university gym in Cincinnati in late May of 2000. My Ohio driver's license and Visa credit card were removed from my wallet and one day later several purchases had been made with the card. I then immediately cancelled the card and then applied for a new driver's license and at this point I assumed that the situation had been resolved and I basically moved on.

I first became aware the next month in June that I had been victimized. I received a letter from Chase Manhattan Bank saying that they had received a suspicious request for credit using my information. I immediately contacted them and got some general information and then contacted the reporting bureaus. I was instructed to place a fraud alert on my file and then I received a credit report.

When I received the report there were approximately eight fraudulent accounts listed on the report. I was very upset and I wanted

to immediately correct the situation but I really did not have any idea how to go about correcting this information. My first instinct was to begin contacting the creditors and speaking to them directly and as I contacted the individual banks, it was not until the fifth bank that I was informed there was actually a process in place to deal with this, so I had to then go back and repeat my conversations with the other banks and prepare the proper documentation for an investigation to be initiated.

It was at this time in the process that I learned that the three reporting agencies operated separately and that I had to go through this process not only once but with all three of them in conjunction. And I found that the information was not always uniform across all three bureaus; there was different information with each one. At the end of my contacting all the reporting agencies I found 13 accounts with a total of $30,000 in credit that had been used, including the purchase of a motorcycle and other sports utility-type goods, as well as purchases at clothing stores, et cetera.

The only thing that linked the perpetrator to my credit was my Social Security number, which was taken from my driver's license. I also later learned that the majority of these applications were done over the phone so the only identification required was the Social Security number. I also received copies of many of the applications with my alleged signature, which did not match up with the signature on my driver's license, and therefore it seems that there was no other verification necessary except for the Social Security number.

I am now extremely careful about sharing this information and I have cautioned my family and friends, as well. However, the damage has already been done. This negative information is very difficult to be removed, as Nicole has testified to. It has been almost a year now and I am still going through the process of contacting people and finding new information on credit reports when I receive them. The process of having this information removed is very heavily weighted against the consumer.

The Fair Credit Reporting Act states that credit-reporting agencies are required to investigate claims of credit fraud and if the claims are supported, remove the false information within 30 days. In October of 2000 I submitted copies of 13 letters and statements from credit-granters stating that the accounts were opened fraudulently and to this day I have not heard back from any of them and my most recent credit report that I pulled, the information was still there and current.

I am left with damaged credit and feel very embarrassed having to explain to my mortgage lender, as I did last week, that I cannot get credit on my house because this information is there that I did not put there. I have paid a very, very high price for the crimes of this one person.

Another problem that has only recently begun to surface is the reappearance of accounts that I had believed to be deleted. I went through the process of having one account removed and then found in my last credit report that the account was still being listed by a collections agency that the account was transferred to. This will initiate another round of doing the investigate reporting that I have had to do in collecting information.

In summary, this experience has been extremely frustrating, tedious and for the most part overwhelming. I have spent countless hours on the phone at home, at work, thinking about it, trying to explain to my wife how we are going to get a house. It has just been a very trying period.

I really hope that this story and our testimony today provides a little bit of insight into some of the realities of identity fraud. Thank you.

Chairman SHAW. Thank you, Mr. Moneme. I also will send a transcript of your testimony to the people you are trying to get a mortgage from. Perhaps that might help.

Mr. MONEME. Thank you.

[The prepared statement of Mr. Moneme follows:]

Statement of Emeka Moneme, Washington, DC

Distinguished Members of the House of Representatives,

Good morning. My name is Emeka Moneme, and I would first like to thank the Subcommittee for the invitation to share my personal experience dealing with identity fraud and specifically, the misuse of my social security number. I hope to convey to you the frustration, anger and violation that comes as a part of this crime, but as I am sure that other victims can attest to, it is something that is difficult to comprehend until it happens to you.

When I try to pull together the circumstances surrounding my information, it appears that the only piece of identification that the perpetrator of this crime had to use was my social security number. My personal property was stolen at the university gym in late May of 2000. My Ohio Driver's License and Visa credit card were removed from my wallet, and one day later, several purchases had been made with the card. I then cancelled the card and applied for a new driver's license. At this point, I assumed that the situation had been resolved and moved on.

I first became aware that I had been victimized in June of 2000. I received a letter from Chase Manhattan Bank, in which they stated that they had received a suspicious request for credit using my information. I immediately called the bank, got some general information and contacted one of the credit reporting agencies. I was instructed to place a fraud alert on my file and a credit report was sent to me.

When I received the report, there were approximately 8 fraudulent accounts. I was upset and wanted to correct the information, but I did not know what to do about them. My first instinct was to begin contacting the credit grantors (banks) to close the accounts. I began this process, but was not until about the fifth bank that I was told that there was a formal procedure for dealing with fraudulently opened accounts. I then had to re-contact all of the banks and prepare the proper documentation to initiate an investigation.

As I began this process, I learned that the three credit reporting agencies operated separately and that I needed to go through the long and tedious process of requesting an investigation with all of the credit agencies. I also learned that the information was not uniform and that they all looked different, so I needed to contact each one. After contacting them all, I identified 13 accounts, with a total of $30,000 in credit.

The only thing that linked the perpetrator to my credit was my social security number, which was taken from my driver's license. I also later learned that the majority of the applications for credit were made over the phone with the social security number as the only identifier. I also received copies of many of the applications, with my alleged signature—none of which matched with the signature on my license. Therefore, it seems that no other verification was done except seeing the social security number.

I am now extremely careful about sharing my personal information, and have cautioned the rest of my family as well. However, the damage has been done. This negative information is very difficult to have removed, even if you have definite proof of wrongdoing. The process for remedying credit is heavily weighted against the private consumer.

The Fair Credit Reporting Act states that credit-reporting agencies are required to investigate claims of credit fraud and if the claims are supported, remove the false information within 30 days. Over the past year, I have submitted several requests for investigations with letters supporting my claim that the account was opened fraudulently. After nearly a year, and countless hours of phone calls, letters,

notaries and credit reports, only 6 accounts have been expunged. I am left with damaged credit, embarrassed as I try to explain away delinquent accounts; and frustrated in my search for financing for a house. I have paid a very high price for the crimes of one person.

Another problem that has only recently begun to surface is the reappearance of accounts that I had believed to be deleted. When credit grantors, write off accounts as a loss, they send them to a collection agency. The collection agency then issues a new number to the account for their records and reports the information to the credit-reporting agency. This then initiates a new round of investigations and paperwork to remove the information.

In summary, this experience has been frustrating, tedious and many times overwhelming. I fully support any action by this subcommittee to protect consumers and their private information. I hope that this story has provided some insight on the realities of identify fraud, and thank you for your time.

Chairman SHAW. And any other place that either you or Miss Robinson might want me to direct your testimony with a cover letter from me.

Mr. Huse, glad to have you with us again.

STATEMENT OF THE HON. JAMES G. HUSE, JR., INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. HUSE. Good morning, Mr. Chairman and members of the Subcommittee.

As you know, my office is charged with protecting Social Security programs from fraud, waste and abuse. No aspect of our mission though is more important than our oversight of the use and unfortunately misuse of the Social Security number or SSN.

In 1935 the SSN was created as part of a new system to track the earnings of employed Americans. Just as no one dreamt that the innocuous nine-digit number would become our de facto national identifier, no one could foresee the breadth and complexity of commerce in the electronic age. Unfortunately, while the SSN and computer technology have matured together, the laws we use to police and protect them have struggled to keep pace.

Misuse of the SSN, catalyzed by the Internet, has quickly become a national crisis. The SSN's universality has become its own worst enemy. The power it wields—the power to engage in financial transactions, power to obtain personal information, the power to create or commandeer identities—makes it a valuable asset and one that is subject to limitless abuse.

It falls on government, which created the SSN and permitted it to assume such power, to take action to control its own creation. Organizations such as the Social Security Administration (SSA) Office of the Inspector General, the Federal Trade Commission and the Department of Justice, have the responsibility to enforce laws designed to protect against SSN misuse and its consequences.

To do so, there must be adequate laws in place. In recent years we have seen the enactment of the Identity Theft and Assumption Deterrence Act of 1998 and the Internet False Identification Prevention Act of 2000. Both are helpful but both treat the disease in its later stages rather than at its onset. Identity theft begins in most cases with the misuse of an SSN and while the ability to pun-

ish identity theft is important, the ability to prevent it is even more critical.

How do we do this? First and foremost, the time has come to put the SSN back in its box. We must make the difficult determinations as to those uses that are appropriate and necessary and those that are merely convenient. The SSN is a unique identifier and its quotidian use as an ID number by schools, hospitals, and other institutions is understandable but dangerous. Its use by Federal, State and local governments not only for taxes and for other legitimate purposes but for everything from drivers licenses to water and sewer bills is a convenience that we can no longer afford.

Its use in private industry, not just for financial transactions but for joining a health club or buying a refrigerator, has become reckless and its ready availability over the Internet must come to a stop.

We need legislation that limits the use of the SSN to those purposes that benefit the holder of the SSN, not the company that sells that person an appliance or the State that issues that person a driver's license. We need legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. And, we need legislation that stops the ready availability of SSNs over the Internet and through other means.

The prevalence of SSN misuse cannot be denied. In fiscal year 2000 our office received over 92,000 allegations. Over half of them, almost 47,000, were allegations of SSN misuse and another 43,000 were allegations of program fraud which, experience has shown us, often includes the potential for SSN misuse.

My office and others, such as the Federal Trade Commission, are doing all we can within the limitations imposed by existing law and resources. We are diligent in referring allegations of identity fraud to the FTC and we conduct investigations of SSN misuse, both program-related and nonprogram-related, on a daily basis. We have conducted undercover operations in which we have purchased counterfeit Social Security cards and reverse sting operations in which we have offered such cards for sale. Several of these cases are now pending in the U.S. Attorney's Offices. We are involved now in a joint investigation with another Federal law enforcement agency in which lists of names and SSNs were being sold to the highest bidder on an Internet auction site. Although the investigation is ongoing and I cannot provide details, I can tell you that we have discovered that the source of the list was a university. This highlights the need to stop the indiscriminate use of SSNs as ID numbers. Unfortunately, while the subject in this case may eventually face criminal charges of some kind, nothing in the Social Security Act prohibits the sale of SSN information.

Our efforts have made a difference but with better laws we can do far more. I welcome this Subcommittee's dedication to this endeavor and attention to this critical issue and I would be happy to answer any questions.

[The prepared statement of Mr. Huse follows:]

Statement of the Hon. John G. Huse, Jr., Inspector General, Office of the Inspector General, Social Security Administration

Good morning, Mr. Chairman, Congressman Matsui, and members of the Subcommittee. As you know, my office is charged with protecting Social Security pro-

grams from fraud, waste, and abuse. No aspect of our mission is more important than our oversight of the use—and misuse—of the Social Security account number, or SSN.

In 1935 the SSN was created as part of a new system to track the earnings of employed Americans. Just as no one dreamt that the innocuous nine-digit number would become our de facto national identifier, no one could foresee the breadth and complexity of commerce in an electronic age. But by 1967, when the Department of Defense abandoned the military identification number in favor of the SSN for armed forces personnel, the theories that would eventually give rise to today's Internet were already being debated. In the quarter century since, the myriad uses of the SSN have continued to expand, while the notion of a worldwide network of computers evolved from theory to reality. Unfortunately, while the SSN and computer technology have matured together, the laws we use to police and protect them have struggled to keep pace.

Misuse of the SSN, catalyzed by the Internet, has quickly become a national crisis. The SSN's universality has become its own worst enemy. The power it wields—power to engage in financial transactions, power to obtain personal information, power to create or commandeer identities—makes it a valuable asset and one that is subject to limitless abuse. It falls on Government, which created the SSN and permitted it to assume such power, to take action to control its own creation. Organizations such as the Social Security Administration, its Office of the Inspector General, the Federal Trade Commission, and the Department of Justice have the responsibility to enforce laws designed to protect against SSN misuse and its consequences. To do so, there must be adequate laws in place.

In recent years, we have seen the enactment of The Identity Theft and Assumption Deterrence Act of 1998 and the Internet False Identification Prevention Act of 2000. The former is the first legislative response to the growing wave of identity thefts and imposes criminal sanctions for those who create a false identity or misappropriate someone else's. The latter closed a loophole left by the first, enabling my office and other law enforcement organizations to pursue those who previously could sell counterfeit Social Security cards legally, by maintaining the fiction that such cards are "novelties," rather than counterfeit documents. Both pieces of legislation are helpful, but both treat the Identity Theft disease in its latest stages, rather than at onset. Identity Theft begins, in most cases, with the misuse of an SSN, and while the ability to punish Identity Theft is important, the ability to prevent it is even more critical.

How do we do this? First and foremost, the time has come to put the SSN back into its box. We as a Government created the SSN, and we as a Government must control it. We must make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient. The SSN is a unique identifier, and its quotidian use as an I.D. number by schools, hospitals, and other institutions is understandable—but dangerous. Its use by Federal, State, and local governments not only for taxes and other legitimate purposes, but for everything from drivers' licenses to water and sewer bills, is a convenience that we can no longer afford. Its use in private industry, not just for financial transactions, but for joining a health club or buying a refrigerator, has become reckless. And its ready availability over the Internet must come to a stop.

We need legislation that limits the use of the SSN to those purposes that benefit the holder of the SSN, not the company that sells that person an appliances or the state that issues that person a drivers' license—legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. I am sensitive to the costs that would be incurred in both the public and the private sectors in implementing the changes that such legislation would require, and I do not suggest that any of us are facing an easy task. Rather, it is a necessary task. The appropriate agencies, in cooperation with governmental authorities and business leaders, must reach an understanding as to the need to limit the use of the SSN and regulations would have to be promulgated reflecting such uses and providing for enforcement mechanisms. In addition, the legislation would need to outlaw the sale of SSNs over the Internet and through other means. With certain legislated exceptions, no private citizen, no business interest, and no ministerial government agency should be able to sell, display, purchase, or obtain any individual's SSN, nor should they be able to use any individual's SSN to obtain other personal information about the individual.

The prevalence of SSN misuse cannot be denied. In Fiscal Year 2000, our office received 92,847 allegations. Over half of them, 46,840, were allegations of SSN misuse, and another 43,456 were allegations of program fraud, which experience has shown us often include implications of SSN misuse. My office and others, such as the FTC, are doing all we can within the limitations imposed by existing law and

resources. We are diligent in referring allegations of Identity Theft to the FTC, and we conduct investigations of SSN misuse, both program-related and non-program-related, on a daily basis. We have conducted undercover operations in which we have purchased counterfeit Social Security cards, and reverse-sting operations in which we have offered such cards for sale. Several of these cases are now pending in U.S. Attorney's Offices. We are involved now in a joint investigation with another Federal law enforcement agency in which lists of names and SSNs were being sold to the highest bidder on an Internet auction site. Although the investigation is ongoing, and I cannot provide details, I can tell you that we've discovered that the source of the lists was a university. This highlights the need to stop the indiscriminate use of SSNs as I.D. numbers. Unfortunately, while the subject in this case may eventually face criminal charges of some kind, nothing in the Social Security Act currently prohibits the sale of SSN information.

In addition to legislation that limits the use of SSNs and provides sanctions for violations, and legislation which criminalizes the sale and purchase of SSN information, it is important to provide an administrative safety net, as well. Our Civil Monetary Penalty program has proven an invaluable asset in the context of SSA program violations when criminal prosecution is not a viable option. Similar authority in the arena of SSN misuse would provide my office with the same ability to take administrative action. I would urge you to consider legislation vesting in us such authority.

With legislation such as that I have discussed, and the continuing dedication of the Government agencies involved, and of this Subcommittee, I am confident that we can reverse the trend of SSN misuse and Identity Theft.

I welcome this Subcommittee's dedication and attention to this critical issue, and I would be happy to answer any questions.

Chairman SHAW. Thank you, Mr. Huse. Mr. Robinson.

STATEMENT OF MICHAEL ROBINSON, SPECIAL AGENT, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. ROBINSON. Thank you, Mr. Chairman and members of the Subcommittee. I will proceed with doing a presentation that will show you the various websites that are available that will assist in facilitating identity theft.

Chairman SHAW. Each of the members has this book, which I believe you have supplied.

Mr. ROBINSON. Yes, sir, Mr. Chairman. Those books will actually be a representation of this presentation here.

As you can see, Mr. Chairman, the first page is a home page on the Internet and this is a first page that is easily accessible and usually the first page that someone will view when they are entering the World Wide Web.

From there they will go to a search engine and there are various search engines out there on the Internet and they could simply type in the type of information they would wish to search for. And as you can see here, we indicated "instant Social Security number searches."

This is one of the sites that actually offers the service to assist an individual in finding Social Security numbers and they also offer a response time anywhere from 15 to 30 minutes. These could actually be purchased over the Internet, this type of service, by anyone with a major credit card and they could instantly receive a response right there over the Internet.

Here, as you can see, a price is listed to actually search for someone's Social Security number, which is $39.95 at this particular site.

Pretty simple information that needs to be put in by anyone. Just input that information there and it just walks an individual through the various steps that they would need to take within this site to complete their search.

Information here that confirms the individual's request, gives them the amount that they will be charged for this particular service. They could have an extensive search and it also lists that the person could actually purchase a one-hour rush to get the Social Security number of an individual.

Here it actually confirms that the purchase has been made, gives you several other selections that the individual can place at this time for other searches, additional information that could be purchased and with this information, the person could assume anyone's identity.

Here is an additional website that is easily accessible, readily available to anyone who has access to the Internet. This site actually offers the same type of service as the previous website that we mentioned.

From here, not only on the Internet could you obtain someone's Social Security card but you could also purchase several identity documents—anything from driver's license to graduation certificates, birth certificates, really the major items that you would need to assume an individual's identity.

As you can see, there are even websites that are available on the Web that actually ranks the top 10 fake ID websites so that if an individual is surfing the Internet looking for places to go and actually obtain a fraudulent identification document or a fraudulent ID, this will give them an idea of what sites are out there and whether or not the sites are worth visiting.

Here we have a fake ID review site. With the fake ID review site, what this does is give an individual an idea of what type of product they would purchase if they would go to the particular sites that are recommended here. It tells you whether or not the products are good, whether or not the products are neutral, where the products are actually made and the time frame in which a person can expect, prior to receiving their fraudulent document in the mail, to include Social Security card, driver's license, birth certificates, things of that nature.

From this website here, as you can see, all 50 States are represented here and with this website you can actually purchase a driver's license from each of the 50 States and with these driver's licenses they could be used as what we call breeder documents. With these driver's licenses here if someone had your name and your address and they knew your Social Security number, depending upon how well the product looks, they could use that to obtain an actual Social Security card with your name and number on it.

Here, as you can see, this site not only offers you a driver's license but once you purchase that driver's license you can also obtain a Social Security card.

This is just the order form for that site, pretty self-explanatory to an individual who is on the Internet, so it is easy to complete.

And once the person completes this application, they can put in their request and obtain the Social Security card and/or driver's license in any name or number they may choose.

On this website here it actually lists the names and Social Security numbers, which have proven to be valid but are not shown in the presentation here, of individuals, a range of individuals from Bill Gates to General Colin Powell to Ted Turner and the heirs to the Wal-Mart chain, as well. Their names and Social Security numbers here are readily available and they are on the Internet as we speak. We have checked that site very recently.

On these various websites that offer you the opportunity to obtain someone's name, Social Security number, they also offer a person, once they obtain that information, the opportunity to apply for, within 15 to 30 seconds, a credit card over the Internet. And once they obtain that credit card it also links you to various sites in which you could instantly start shopping with that information while you are there on the Internet.

Mr. Chairman and members of the Subcommittee, this would conclude the presentation. Other than the driver's license and the Social Security number that, Mr. Chairman, I think you have before you, those are driver's licenses and Social Security numbers that can actually be purchased over the Internet. And, as you can see, there is an adhesive sticker on both of those identification documents that could easily be removed and once it is removed there is no indication that the sticker was ever there.

[The prepared statement of Mr. Robinson follows:]

Statement of Michael Robinson, Special Agent, Office of the Inspector General, Social Security Administration

The following was a PowerPoint presentation:

Slide 1

Slide 2

Next Page

Home | Shopping | Dogpile Destinations | Help

DOGPILE Metasearch Results

instant social security number searches Fetch

Select: The Web

amazon.com Best Sellers

FDIC insured.

Bookmark this page with Flink • Buy books about "instant social security number searches" at Amazon.com • Research "instant social security number searches" at Electric Library

Are you looking for: Social Security Number Searches

Find results for "instant social security number searches" on the Yellow Pages!

Dogpile Suggests: Bank Online with Silicon Investor Banking Center, powered by National InterBank. Open an account and enjoy No Fee Banking with Great Rates, Free Online Bill Pay and more!

Web | Images | Audio | Auction | News | FTP | Discussion | Multimedia |

Search engine: GoTo.com found 10 results. The query sent was +instant +social +security +number +searches

1. 99% Social Security Number Tracing - Search Information - National Credit Information Network -
~ ...using a Social Security Number find the names and addresses associated with the ssn. How to find people, skips and verify who people say they are.
www.myrtlebeachrental.com

2. how to locate a cellular phone number, pager number, telephone number, p.o. box identity, phone bills, and dmv records
Instant Access Investigative private web site. Compile your own profile on anyone or any business
www.hitekinfo.com

3. USSEARCHit, Get public records & fast searches, instant free search links
USSEARCHit, Get public records & fast searches, instant free search links, locate, people, property, business, credit, birth, death, criminal, ssn, records, Investigators, skiptracing
www.ussearchit.com

Slide 3

4. USSEARCHit, Get public records & fast searches, instant free search links
USSEARCHit, Get public records & fast searches, instant free search links, locate, people, property, business, credit, birth, death, criminal, ssn, records, Investigators, skiptracing
ussearchit.com

5. net detective
net detective, become your own private investigator, investigate anyone
respondpro.com

6. Investigative Private Web Site
Instant Access Investigative private web site. Compile your own profile on anyone or any business
www.usatrace.com

7. Investigative Private Web Site
Instant Access Investigative private web site. Compile your own profile on anyone or any business
refer.ccbill.com

8. SearchBug -> PeopleFinder -> Social Security Number
This tool will tell you if your Social Security Number is valid and the time period and the state it was issued
www.searchbug.com

9. Free People Searches / Social Security & Genealogy Information. Locate lost friends and relatives.
Free people and geneology searches. Social security information
www.new-web.com

10. DRIVING
PRICING: The pricing quoted on this price list for Instant Data Return searches includes a $3 Database Access Fee. This fee will be charged in the event that no record is found on searches noted by two asterisks (**). Snapshot Reports
www.tracersinfo.com

Go to Goto.com for more results

Search engine: LookSmart found 0 results. The query sent was +instant +social +security +number +searches

Search engine: FindWhat.com found 0 results. The query sent was instant social security number searches

Slide 4

Search engine: Spinks by About **found 10 results.** The query sent was +instant +social +security +number +searches

1. Get Unclaimed Money or Property You're Entitled To
Find out if you're one of millions of Americans entitled to receive unclaimed property or money
http://financialplan.about.com/library/weekly/aa121000b.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

2. Scam Alerts - Tom's Editor's Dozen - Contesting and Sweepstakes
Scam Alerts - Tom's Editor's Dozen
http://contests.about.com/library/blscams13.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

3. Cyber-Smart Parents
Cyber-Smart Parents
http://kidsparents.about.com/library/weekly/aa031599.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

4. MacSurfer's Headline News™
MacSurfer's Headline News: THE Mac Portal Nonpareil
http://www.macsurfer.com/

5. Calculators - page 2 of 3
Financial calculators for budgeting, home buying, car buying, loans, investing, savings, retirement, and more,
http://financialplan.about.com/cs/calculators/index_2.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

6. Let Your Coffee Do the Computing: An overview of quantum computing - Artificial Intelligence - 06/15/97
Quantum computing can be done and is being done. It's only a matter of time before we have access to unlimited computing power, from your About.com Guide
http://ai.about.com/library/weekly/aa061597.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

7. Email Petitions, Politics and Protest
Rage and pointlessness on the Internet
http://urbanlegends.about.com/library/bl.protest.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

8. Intelligent Machine Post and Ellis's Endangered Employment Katalog - Artificial Intelligence - 04/05/98
AI newsletter and compendium of jobs threatened by AI, from your About.com Guide
http://ai.about.com/library/weekly/aa040598.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

9. Bush - Gore Debate: Money - Social Security
Transcript of the October 3, 2000 Bush - Gore debate.
http://usgovinfo.about.com/library/weekly/aa100600e.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

Slide 5

10. Archives of

http://immigration.about.com/library/bl.HeadlineArchives1999.htm?am=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

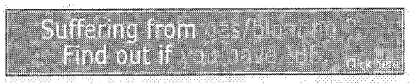
Go to Spinks for more results

Search the next 13 engines or try the Dogpile Directory.

Next

Dogpile Suggests: Bank Online with Silicon Investor Banking Center, powered by National InterBank. Open an account and enjoy No Fee Banking with Great Rates, Free Online Bill Pay and more!

Are you looking for: Social Security Number Searches



• Buy books about "instant social security number searches" at Amazon.com • Research "instant social security number searches" at Electric Library

DOGPILE Metasearch Results

instant social security number searches Fetch!

Select: The Web

Traded on NASDAQ: INSP © 1996-2000 InfoSpace, Inc. All Rights Reserved.
Terms of Use | Privacy Policy | Customer Feedback | About InfoSpace

Slide 6

Next Page

Home | Shopping | Dogpile Destinations | Help

DOGPILE Metasearch Results

instant social security number searches Fetch!

Select: The Web

amazon.com Best Sellers

Bookmark this page with Blink · Buy books about "instant social security number searches" at Amazon.com · Research "instant social security number searches" at Electric Library

Are you looking for: Social Security Number Searches

Find results for "instant social security number searches" on the Yellow Pages!

Dogpile Suggests: Bank Online with Silicon Investor Banking Center, powered by National InterBank. Open an account and enjoy No Fee Banking with Great Rates, Free Online Bill Pay and more!

Web | Images | Audio | Auction | News | FTP | Discussion | Multimedia |

Search engine: GoTo.com found 10 results. The query sent was +instant +social +security +number +searches

1. %% Social Security Number Tracing - Search Information - National Credit Information Network -
~ ..using a Social Security Number find the names and addresses associated with the ssn. How to find people, skips and verify who people say they are.
www.myrtlebeachrental.com

2. how to locate a cellular phone number, pager number, telephone number, p.o. box identity, phone bills, and dmv records
Instant Access Investigative private web site. Compile your own profile on anyone or any business
www.hitekinfo.com

Slide 7

3. USSEARCHit, Get public records & fast searches, instant free search links
USSEARCHit, Get public records & fast searches, instant free search links, locate, people, property, business, credit, birth, death, criminal, ssn, records, Investigators, skiptracing
www.ussearchit.com

4. USSEARCHit, Get public records & fast searches, instant free search links
USSEARCHit, Get public records & fast searches, instant free search links, locate, people, property, business, credit, birth, death, criminal, ssn, records, Investigators, skiptracing
ussearchit.com

5. net detective
net detective, become your own private investigator, investigate anyone
respondpro.com

6. Investigative Private Web Site
Instant Access Investigative private web site. Compile your own profile on anyone or any business
www.usatrace.com

7. Investigative Private Web Site
Instant Access Investigative private web site. Compile your own profile on anyone or any business
refer.ccbill.com

8. SearchBug -> PeopleFinder -> Social Security Number
This tool will tell you if your Social Security Number is valid and the time period and the state it was issued.
www.searchbug.com

9. Free People Searches / Social Security & Geneology Information, Locate lost friends and relatives.
Free people and geneology searches. Social security information.
www.new-web.com

Slide 8

10. DRIVING
PRICING: The pricing quoted on this price list for Instant Data Return searches includes a $3 Database Access Fee. This fee will be charged in the event that no record is found on searches noted by two asterisks (**). Snapshot Reports
www.1tracersinfo.com

Go to Goto.com for more results

Search engine: LookSmart found 0 results. The query sent was +instant +social +security +number +searches

Search engine: FindWhat.com found 0 results. The query sent was instant social security number searches

Search engine: Spinks by About found 10 results. The query sent was +instant +social +security +number +searches

1. Get Unclaimed Money or Property You're Entitled To
Find out if you're one of millions of Americans entitled to receive unclaimed property or money
http://financialplan.about.com/library/weekly/aa121000b.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

2. Scam Alerts - Tom's Baker's Dozen - Contesting and Sweepstakes
Scam Alerts - Tom's Baker's Dozen
http://contests.about.com/library/biscams13.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

3. Cyber-Smart Parents
Cyber-Smart Parents
http://kidspenpals.about.com/library/weekly/aa031599.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

4. MacSurfer's Headline News™
MacSurfer's Headline News: THE Mac Portal Nonpareil
http://www.macsurfer.com/

Slide 9

5. Calculators - page 2 of 3
Financial calculators for budgeting, home buying, car buying, loans, investing, savings, retirement, and more.
http://financialplan.about.com/cs/calculators/index_2.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

6. Let Your Coffee Do the Computing: An overview of quantum computing - Artificial Intelligence - 06/15/97
Quantum computing can be done and is being done. It's only a matter of time before we have access to unlimited computing power, from your About.com Guide
http://ai.about.com/library/weekly/aa061597.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

7. Email Petitions, Politics and Protest
Rage and pointlessness on the Internet
http://urbanlegends.about.com/library/blxprotest.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

8. Intelligent Machine Post and Ellis's Endangered Employment Katalog - Artificial Intelligence - 04/05/98
AI newsletter and compendium of jobs threatened by AI, from your About.com Guide
http://ai.about.com/library/weekly/aa040598.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

9. Bush - Gore Debate Money - Social Security
Transcript of the October 3, 2000 Bush - Gore debate.
http://usgovinfo.about.com/library/weekly/aa100600e.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

10. Archives of

http://immigration.about.com/library/blHeadlineArchives1999.htm?iam=dpile&terms=%2Binstant+%2Bsocial+%2Bsecurity+%2Bnumber+%2Bsearches

Go to Spinks for more results

Slide 10

Search the next 13 engines or try the Dogpile Directory.

Next

Dogpile Suggests: Bank Online with Silicon Investor Banking Center, powered by National InterBank. Open an account and enjoy No Fee Banking with Great Rates, Free Online Bill Pay and more!

Are you looking for: Social Security Number Searches

Suffering from [illegible]
Find out if [illegible]

Buy books about "instant social security number searches" at Amazon.com · Research "instant social security number searches" at Electric Library

DOGPILE Metasearch Results

instant social security number searches | Fetch

Select: The Web

Gladiator
Chicken Run
Meet the Parents
Nutty Professor II

FREE DVDs After Rebate

CyberRebate SHOP NOW

Traded on NASDAQ: INSP © 1996-2000 InfoSpace, Inc. All Rights Reserved.

Terms of Use | Privacy Policy | Customer Feedback | About InfoSpace

Slide 11

Next Page

Search to find people, locate property, find court, phone, vehicle & public records – free search info!

USSEARCHIT.COM

The information you need Now with No unnecessary waiting & No registration fee or sign-up required!

| Contact Information | Feedback | Support | Home |

Congratulations! You've found the one place to find, locate, trace or track down anybody! We offer locate searches, DMV driver & vehicle searches, telephone record searches, financial searches, plus criminal records, civil & court records, property records, P.O. box traces, & free searches

Link

Affiliate Program

Licensed Private Investigators

Click here to join our Affiliate Program & start earning cash today!

As low as 2.99% Intro A.P.

30 second approval. Apply now!

Need an Investigator?

Click here!

Try our sample people search!

ORDER MENU

PEOPLE SEARCHES

Locate by name
Locate by previous address
Locate by SSN number
Find SSN (Restrictions apply)
Advanced people search
Full Skip-trace for current address

Click here to find people *FAST*

Why go anywhere else?

We are a licensed Investigative Agency employing experienced Investigators. We not only provide you the information you need *when you need it*, but we also *guarantee results* & protect your identity, which is always *strictly confidential*.

We offer:

- *Low rates & Quick turnaround times*
- *Accurate & professional reporting*
- *No signup or up front fee's*
- *Personal service*
- *Order by Net, phone or fax*

Slide 12

Current employment search
Find date of birth
National Death Records

ASSET SEARCHES

Business Records & Filings
Financial Records
Real Estate record search
Bankruptcy & judgments

TELEPHONE SEARCHES

Listed telephone number search
Unlisted telephone number search
Search for number by address
800-900 number search
Pager beeper search
Pay telephone number search
International Phone Directory

PUBLIC RECORDS

Workers Compensation Records
Criminal record search by county
Statewide criminal record search
National Felony Wants & Warrants
Full criminal record search

VEHICLE RECORDS

Statewide driver history

Compare our fees... BUY HERE, SAVE HERE!

SERVICE	OUR FEE	COMPETITORS FEE	YOU SAVE $
Locate by SSN Number	$27.95	$39.95	$12.00 (30 %)
Locate by Previous Address	$29.95	$39.95	$10.00 (25 %)
Locate by Name	$29.95	$49.95	$20.00 (40 %)
Full Skip-Trace	$149.95	$205.00	$55.05 (35 %)

These are just a few examples of our savings, but you can expect to save around 30% on most all of our searches all the time!

Whatever your information needs, you can count on us to deliver!

Available Services:

- Fraud Investigations
- Accident Reconstruction
- Surveillance
- Skip-tracing & locating people
- Finding debtors & deadbeats
- Find old classmates, friends & lost loved ones
- Identify assets & property
- Complete background checks
- Pre-employment screening
- Public criminal, civil & court records
- Driver and vehicle history
- Business Records, credit reports, & filings

Slide 13

Vehicle records
Search for drivers license number

CUSTOM SEARCHES AVAILABLE

Law Enforcement & Corporate discounts available
Call for details

(614) 491-9830

Visit Our Affiliate @
PRICELINE.COM

Always strictly confidential

PEOPLE SEARCH

Last name:
First name:
Date of birth:
Social security#: ###-##-####
State to search: Select State
Approx age:
e-mail address:
May we notify you of special offers and promotions? yes
Go get it!

We Support the National Association of Investigative Specialist

Doctor Faces Fraud Charge In OxyContin Investigation | FraudNews.com

Top

©1999-2001 - All rights reserved

| Contact Information | Feedback | Support |

Click here to start accepting credit cards on your site today!

Slide 14

Next Page

Search to find people, locate property, check court, photo, vehicle & public records + free search tools!

US SEARCH IZ.COM

The information you need 24/7 with 2/7 minute service waiting & 2/7 registration fee or sign-up required!

| Contact Information | Feedback | Support | Home |

Congratulations! You've found the one place to find, locate, trace or track down anybody! We offer locate searches, DMV driver & vehicle searches, telephone record searches, financial searches, plus criminal records, civil & court records, property records, P.O. box traces, & free searches

29 Categories

Office Manager

Licensed Private Investigators

Click here to join our Affiliate Program & start earning cash today!

As low as 2.99% Intro APR

30 second approval... Apply now!

Need an Investigator?

Click here!

Locate Social Security Number

Search Price: $39.95

Availability: National

Approximate Return Time: 15-30 minutes during business hours (MON - SAT)

Requires: Subject's Name & current or previous address & lawful purpose

*DENOTES REQUIRED FIELD

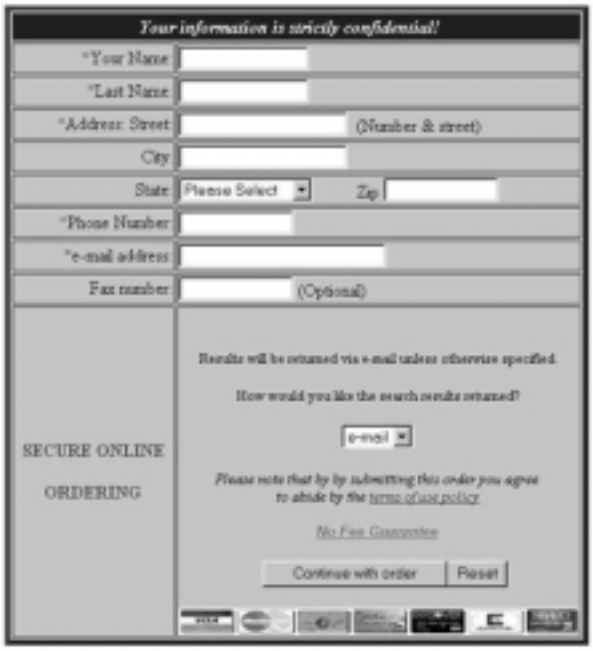
Slide 15

PLEASE ENTER AS MUCH INFORMATION AS POSSIBLE.

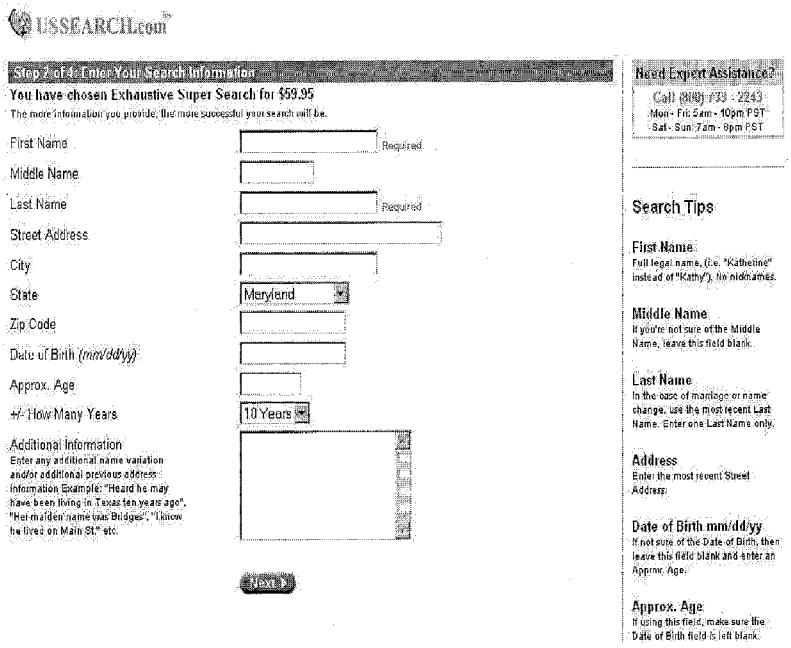
Social Security Number Search

*Subject's First Name	
*Subject's Last Name	
Middle initial (if known)	
Date of birth (if known)	
*Address: Number & street	Apt# (If Applicable)
City	
State	Please Select
Zip	
Additional Comments Regarding This Search	
*Legal purpose for search	Select One From List

Slide 16



Slide 17



Slide 18

Next Page

USSEARCH.com™

Step 4 of 4: Please review and confirm your order

You are searching for:

First Name
Last Name
Street Address
City
State
Zip Code
Date of Birth
(+/-) How Many Years

Edit

Billing Summary :

First Name
Last Name
Billing Address
City
State
Zip Code
E-mail Address

Success Stories

"At first I tried to use the "free" search databases on the Internet. However, after a couple of hours I saw that I was running around in circles, and their data was either incorrect or lacking. You located the individual that I was seeking, and even supplied me with a correct phone number. Thanks a million." *M.S.*

"Dear US Search. WOW, how you changed our lives. Last night I went on your web site and in less than an hour you found my sister.... after 34 years !!!! You're THE GREATEST. I will never forget how YOU put together our family. I will also pass on the good word for you if ANYONE I ever meet needs to search for anyone!!!! Blessings to ALL!" *G.G.*

"My only regret is that it took me so long to contact US SEARCH. I should have called years ago. It was so easy. I found my best friend from high school. Thank you." *- Ann H.*

"Thanks to a US SEARCH Public Record Report, I settled a wrongful eviction action on behalf of tenants against their landlord." *- Andrew W., Attorney-at-law.*

Slide 19

Edit

Product Ordered:	
Exhaustive Super Search	$19.95
1 Hour Rush	$25.00
TOTAL	$44.95

Submit Order

Any information provided is strictly confidential (see Privacy Policy). By placing this order, you accept all Terms and Conditions contained in the US SEARCH.com Inc. Consumer Services User Agreement. Please allow 20 to 40 seconds for us to process your credit card.

Home | Contact Us | News & Events | Investor Info | Privacy Policy

© US SEARCH.com Inc. 1996-2001 All Rights Reserved.

Slide 20

USSEARCH.com™

Order Confirmation

Thank you for your order from US SEARCH.com
Your Order Reference Number is: 55360434

Items Ordered

Product	Price
Exhaustive Super Search	$59.95
1 Hour Rush	25.00
Current Search Charges	$84.95
Total Charge For All Searches	**$84.95**

The information you have submitted has been received and the results of your search will be returned to: onthewebsurfing@yahoo.com. Instant Search Results are NOT Emailed!

Congratulations! Save up to 25% on your next purchase right now!
In appreciation of your order, you now qualify for discounts on the valuable services below.
Don't Wait! This offer only applies during this session.

Discounted Searches

PRODUCT		DISCOUNTED PRICE	CHOOSE
People Locate Search	Sample Report	was ~~$31.95~~ Now $35.95	◉
Exhaustive Super Search	Sample Report	was ~~$59.95~~ Now $53.95	○
Super Search	Sample Report	was ~~$49.95~~ Now $44.95	○
On-Premise County Courthouse Search	Sample Report	was ~~$29.95~~ Now $26.95	○
Due Diligence (Consumer)	Sample Report	was ~~$295~~ Now $265.50	○
Instant Death Records Search	Sample Report	was ~~$12~~ Now $9.00	○
Department of Corrections Search	Sample Report	was ~~$34.95~~ Now $27.95	○
Sex Offender Search	Sample Report	was ~~$34.95~~ Now $27.95	○

Next >

If you have further questions, please contact Customer Service by cservice@ussearch.com, or via phone at: (877) 327-2460, 5am -

Slide 21

Next Page

People
Assets
Addresses
Phone Numbers

Unlisted Phone Numbers Etcetera

We take the stress out of the unknown when you...

"We are a Powerful Information Location Machine"

About Us | Sample Search | Testimonials | Russia Backgrounds | Mail Order Option

USA & Canada Information Searches & Traces

• PEOPLE SEARCH	• Unlisted Phone Numbers	• Reverse Unlisted Phone Searches
• SSN or SIN Trace	• Vehicle Trace	• 800-900 #'s
• P.O. Box Trace	• Disconnected Phone Trace	• Basic SSN or SIN Lookup
• Name Header Search	• Bankruptcy Trace	• Professional License Lookup
• Comprehensive Background	• Cell Phone Reverse	• Pager Number Reverse
• Criminal Records Check	• Employment Verification SSN	• National FBNs & Business Filings
• Divorce Documents	• CANADA	•

Authorized Purpose: [(Choose One)]
Select Authorized Purpose from the above List

We assist attorneys and other professionals daily.
We provide a confidential & personal service not found elsewhere.
Please do not hesitate to contact us before ordering any search.
We want you to be perfectly comfortable about who you are dealing with.
Please do not Order a search with any credit card other than your own!

Slide 22

Please read our terms and conditions prior to requesting your service.
Click on the #S Header Line to order each specific search.
Available for U.S.A. & NEW CANADA!

Special

-- USA Special! --

#S16 - USA People Finder Search

Click Here to Order USA

Canadian Searches-Click Here

You Supply: **Subjects Name and past address (and /or) SSN/SIN: You may supply just one or all three.**

This search provides: The latest address on the subject, verify an address on an applicant, locate a missing person, obtain previous addresses for seven years, obtain aliases used and determine if the subject has used more than one SSN/SIN number.
This is the most complete listing of current and archived names, addresses, and dates of birth **available anywhere**. We have access to over 50 million unlisted households that **do not** appear in our competitors' data.

Search Details:
Cost of USA People Finder Search ~~$35.00~~ SPECIAL = $29.00

Canadian Searches - $57.00 - Click Here
(You will not find this search anywhere else!)

Please allow 1-3 business days - to complete the National People Finder Search
U.S.A. & NEW CANADA

Slide 23

Unlisted

#S1- Unlisted Phone Number Searches

Click Here to Order

You Supply: **Subjects Address** Be Certain you include ALL street identifiers such as: Avenue, Street, Drive. If it is an apartment building, you MUST supply the apartment number.

We Return: **Unlisted Phone number**: The resident's name & all telephone numbers active at that location.

Search Details:
Cost of Unlisted Telephone Number Search: $80.00
Please allow 3-5 business days - to complete Unlisted Telephone Number Search
Accuracy GUARANTEED - No Information / No Charge!
All U.S.A. & NEW CANADA

Reverse

#S2- Unlisted Phone Search Reverse

Click Here to Order

You Supply: **Subjects unlisted telephone number** / non-published telephone
We Return: Subjects Name and Physical Address

Slide 24

Search Details:
Cost of Unlisted Telephone Number Search: $80.00
(This does not include cell phones or pagers)
Please allow 3-5 business days - to complete Unlisted Telephone Number Search
Accuracy GUARANTEED - No Information / No Charge!
All U.S.A. & NEW CANADA

SSN

#S3 - Social Security Search

Click Here to Order

You Supply: **The Social Security Number** (and any other information you have such as a name or DOB)

We Return: SSN/SIN Verification
The subject(s) who have been reported to use the social security number
AKA's (alias used) reported
Their last reported addresses with dates reported back 10 years (or more)
Their D.O.B.
Listed Phone Numbers for Subject's Addresses
Other People who possibly live at Subject(s) address
Other people associated with Subject's SSN/SIN
Other Misc. Information

Search Details:
Cost of Social Security Number Search: $57.00
Please allow 0-3 business days - to complete Social Security/Insurance Number Search
U.S.A. & NEW CANADA

vehicle

Slide 25

#S4 - Vehicle Tag Search

Click Here to Order

You Supply: **STATE & Vehicle Tag** or Vehicle Identification Number (VIN)

We Return: All Information on File From DMV - Pertaining to the Vehicle, Registered Owner and Lien Holder

Search Details
Cost of DMV Search: $125.00

This search is now available for all states except CA for license number.

Please allow 3-5 business days to complete search
U.S.A. Only

800

#S5 - 800/888/900 Numbers Name & Address Search

Click Here to Order

You Supply: **The Number to be searched**

We Return: The Owners Name and Address

Search Details: Cost of Search: $125.00
Please allow up to 10 business days (normally 3 business days) to complete Search
Accuracy GUARANTEED - No Information / No Charge!
USA & NEW CANADA

Slide 26

po box

#S6 - Physical Address to a P.O. Box Search

Click Here to Order

You Supply: **The subjects name**
The post office box number
The zip code

We Return: The subjects physical address of record from the post office

Search Details Cost of Post Office Box Search: $125.00
Please allow 3-5 business days to complete search
Accuracy GUARANTEED: No Information - No Charge!
USA Only

---

disconnect

#S7 - Disconnected Telephone

Click Here to Order

You Supply: **The disconnected telephone number**

We Return: Name & Service Address
Forwarding Address & NEW Phone Number (if active with same carrier)

Slide 27

Search Details

Cost of Disconnected Telephone Search: $85.00
Phone may not have been disconnected for more than three months!
Please allow 3-5 business days to complete Disconnected Telephone search
(This does not include cell phones or pagers)
Accuracy GUARANTEED: No Information - No Charge!
U.S.A. & NEW CANADA

---

basic

#S8 - Social Security/Insurance Trace

Click Here to Order

You Supply: **Submit subjects SS number & Name.**

We Return: The name associated with the SSN and chronological address history. The latest address reported on the subject. Used to verifiy an address on an applicant, locate a missing person, obtain previous addresses for seven years, obtain aliases used and determine if the subject uses more than one SS number.

Search Details

Cost of Social Security Trace: $35.00
Please allow 3-5 business days to complete search (usually returned same business day)
USA only

Slide 28

Name

#S9 - Name Header Search

Click Here to Order

You Supply: **Name & State**

We Return: A name and any variations of the name including aka's, latest and past addresses and the date the addresses were reported, an age or date of birth and sometimes a phone number. The search is nationwide.

Search Details:

Cost of Name Header Search: $35.00
This search takes 1 - 3 business days.
This is a very good search if you have very little to go on.
U.S.A. Only

NEW

#S12 - Triple Merge SSN# Trace/Search

Click Here to Order

You Supply: **Submit subjects name and Social Security Number**

We Return: The most current name & address on file with **all three major credit repository services**. It also includes : aliases reported, address listings back to 10 years, DOB, driver license number & state of issue (where allowed by law) , SSN origin & issue date, fraud alert, list of neighbors name, address & phone numbers.

A powerful tool to locate most current address for a subject or to determine SSN Fraud. Some information may not be available for every record.

Slide 29

Search Details

Cost of Search: $80.00
Please allow 3 business days to complete search
U.S.A. Only

Pro

#S14- Professional License Search

Click Here to Order

You Supply:**Subjects Name and License number (If available)**

We Return: Subjects License Status, ; the license holders name and address, if they are deceased, license type and number, degree, date of issue, date of expiration, and any Disciplinary Actions taken against a medical doctor. Information varies from state to state.
(Does **not** include these states - IL,KY,LA,MC,MO,NV,ND,PA,SC,WV and WI)

Search Details:
Cost of Search: Medical License Search $20.00
Please allow 3-5 business days - to complete Medical license Search
USA Only

Slide 30

#S16 - National People Finder Search

Click Here to Order

You Supply:**Subjects Name and a past address and /or SSN:**

This search provides: The latest address on the subject, verify an address on an applicant, locate a missing person, obtain previous addresses, obtain aliases used and determine if the subject has used more than one SSN number.
We access over 50 million unlisted households that **do not** appear in our competitors' data.
Search over 1 Billion records. This is the most complete listing of current and archived names, addresses, phone numbers, and dates of birth **available anywhere.**

Search Details:
Cost of National People Finder Search ~~$35.00~~ SPECIAL = $29.00
Please allow 3-5 business days - to complete National People Finder Search
USA & NEW CANADA

Bank

#S17 - Bankruptcy Search

Click Here to Order

You Supply:**Subjects Name & SSN# & State:**

We Return: Search of over **9.5 million records of virtually every bankruptcy filing from 1/1/92 to current.** Every record includes full names with some addresses and in most cases *full docket reports.* Additional data fields include: attorney and trustee names, type of filing (chapter 7 or 11, etc.), status of filing (dismissed or discharged, etc.), dollar amount, hearing dates and more. This is a huge source of information.

Slide 31

Search Details:
Cost of National Bankruptcy Search $35.00
Please allow 3-5 business days - to complete Bankruptcy Search

U.S.A. Only

---

background

#S18- Comprehensive Background Profile

Click Here to Order

You Supply: **Subjects Name & Address OR SSN**

We Return: Verification of information related to the Social Security Number including, when available,
current address information from the three major consumer reporting agencies,
historical address information,
year/date of birth, information related to social security numbers,
listed phone numbers
Liens & Judgments,
Bankruptcies,
Property Ownership including Real property,
Deed Transfers,
UCC Lien Filings,
Professional Licenses Sweep, Selective Service/for dob after 1959
Relatives & others possibly living at same address,
AKA's & possible other Social Security Numbers
Spouses in the states of Florida and Texas, and state-specific databases.
Criminal Records Check

Slide 32

This information is derived from a spectrum of databases so it provides a solid overview of the subject of your search.

Search Details:
Cost of Background Profile: $100.00
Please allow 3 - 10 business days (normally 3 days) to complete Profile.
U.S.A. Only

Cellular Phone

#S20 - Cellular Phone Reverse

Click Here to Order

You Supply: **Cellular Phone Number**

We Return: Users name and current address

Search Details:
Cost of Cell Phone Trace: $125.00
Please allow 3 - 10 business days (normally 3 days) to complete Cell TraceSearch

All U.S.A. & CANADA

Slide 33

Pager

#S21 - Pager Reverse

Click Here to Order

You Supply: **Subjects Pager Number**

We Return: Users name and current address.

Search Details:
Cost of Pager Trace: $125.00
Please allow 3 - 10 business days (normally 3 days) to complete Cell TraceSearch

---

Criminal

#S23 - Criminal Records Check

Click Here to Order

You Supply: **Subjects full name and address and SSN if available**

We Return: Criminal records on file with the US Government including federal, civil and appellate courts. Will return bankruptcies. (Will not return DUI's if older than 3 years.)

Search Details:
Cost of Criminal Records Check: $35.00
Please allow 3 - 5 business days (normally 3 days) to complete Criminal Records Check

Slide 34

SSN Sweep/Employment Verification Check

#S22 - SSN Sweep

Click Here to Order

You Supply: **Subject's SSN**

We Return: Subjects using SSN with address history.
Use for employment verification. Also checks SS Death Index for bogus number. Returns State issued and year issued. Returns ALL people associated with SSN given.

Search Details:
Cost of SSN Sweep: $25.00
Please allow 3 business days (normally same day) to complete SSN Sweep

fbn

#S24 -National FBNs & New Business Filings

Click Here to Order

You Supply: **Business name and state, street address and person's name if available**

We Return: New business filing records. Information is obtained from government filing offices such as Secretaries of State, Fictitious and Assumed Name Filings, Boards of Equalization and various licensing offices.

Slide 35

Search Details:
Cost of New Business filings: $35.00
Please allow 3 business days (normally same day) to complete New Business Sweep

To order a search by check or money-order - Send the appropriate amount to:

Investigative Resources
P.O. Box 1466
International Falls, MN 56649

Include a number to have the report faxed to you or a return address for it to be mailed to. Include everything you know about your request/subject and provide a valid email address so we may contact you and/or email you the report if you choose that method. A money-Order request is processed same day. (A check needs to clear the bank first so is slower.)

By requesting any search on this site you signify your agreement to use requested information for legitimate purposes only, and to hold harmless and indemnify Investigative Resources & its owner.

More Searches Coming Soon!

About Us

Need Help? Have a Question? Email us here!
Investigative Resources

USA
Investigative Resources

Slide 36

P.O. Box 1456
International Falls, Minnesota
56649

International
1105 1st Street East
Fort Frances, Ontario, CANADA
P9A1M1
807-481-2593
mailto:cusfsup@investigative.on.ca

Search

HostingOwl "The wise way to search the web"

We support anti-stalking laws. **We do require** that you supply a valid reason for your request in the form of a statement in your email order to us such as: Child support enforcement, Criminal suit location, business affiliations, etc...as set forth by the fair trade commission.

TERMS & CONDITIONS: **All orders, once submitted, are non-cancelable. All information obtained by us, or by our affiliates, is intended for legitimate and lawful use only; by proceeding forth with this information request, you (the client), agree to indemnify, hold harmless, protect and defend (in a court of law) Investigative Resources and/or it's affiliates if the information is misused in any way. We reserve the right to refuse service to anyone at anytime for any reason.**

CREDIT CARD FRAUD IS A SERIOUS OFFENSE!

WHAT CONSTITUTES CREDIT CARD FRAUD? Using your credit card to obtain goods or services and then claiming that you did not authorize the transaction, that you have no idea what the charge is for or falsely claiming that the card number was stolen as well as making any other claim or statement regarding card usage which is not true. Worse yet, using someone else's credit card!

Slide 37

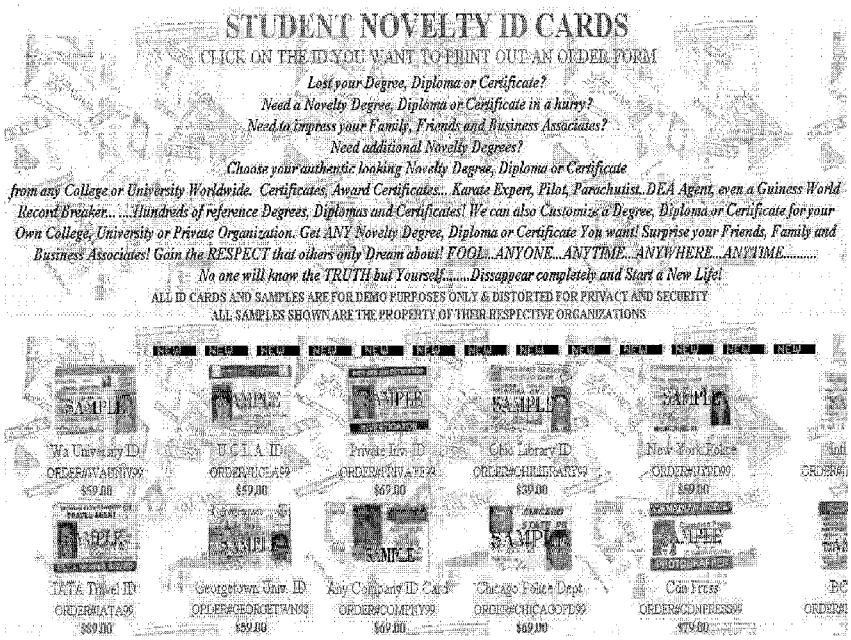
WELCOME TO MORE SAMPLES OF OUR REAL NOVELTY ID CARDS AND CERTIFICATES

Zoom in to get a closer view of any ID. card.
Click on your right mouse button and select
VIEW IMAGE
CLICK GO BACK BUTTON TO RETURN TO THIS PAGE
Click on any ID to place your order and go straight to our
ORDER FORM
Order our version of these
REAL NOVELTY ID CARDS BY
CLICKING ON THE ID OF YOUR CHOICE
THE MOST REALISTIC NOVELTY ID CARDS
AVAILABLE ANYWHERE IN FULL COLOR

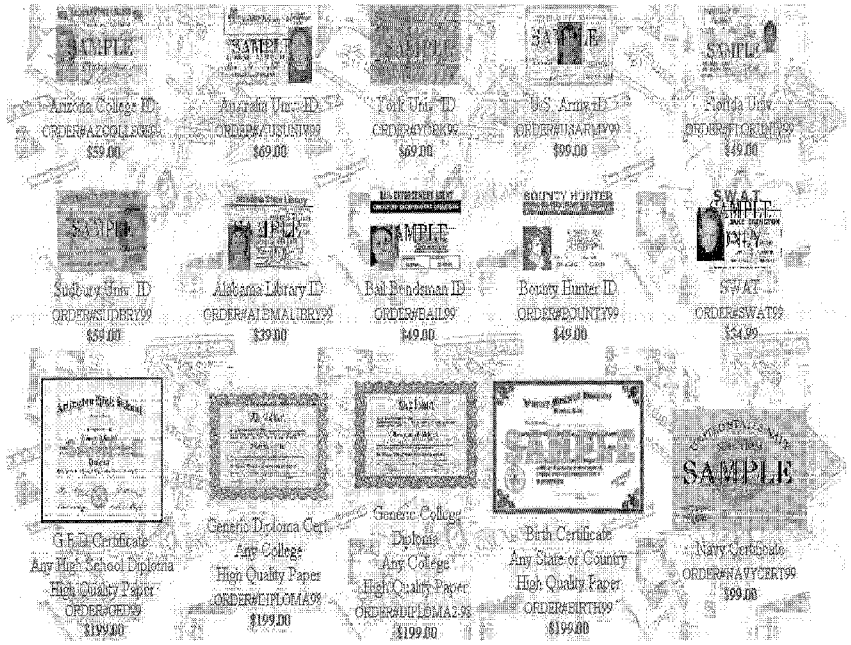
Thank you for your patience while we load these
REAL NOVELTY ID SAMPLES

WE ARE THE ONLY ID COMPANY WHO
CAN OFFER YOU AN AUTHENTIC LOOKING HOLOGRAM FOR ANY STATE PROVINCE OR COUNTRY
ADD AN AUTHENTIC HOLOGRAM TO ANY ID FOR ONLY $44.00
OR A EVEN MORE GENUINE VALID HOLOGRAM SEAL OF AUTHENTICITY FOR $88.00
RAISED SEALS FOR CERTIFICATES ONLY $89.00

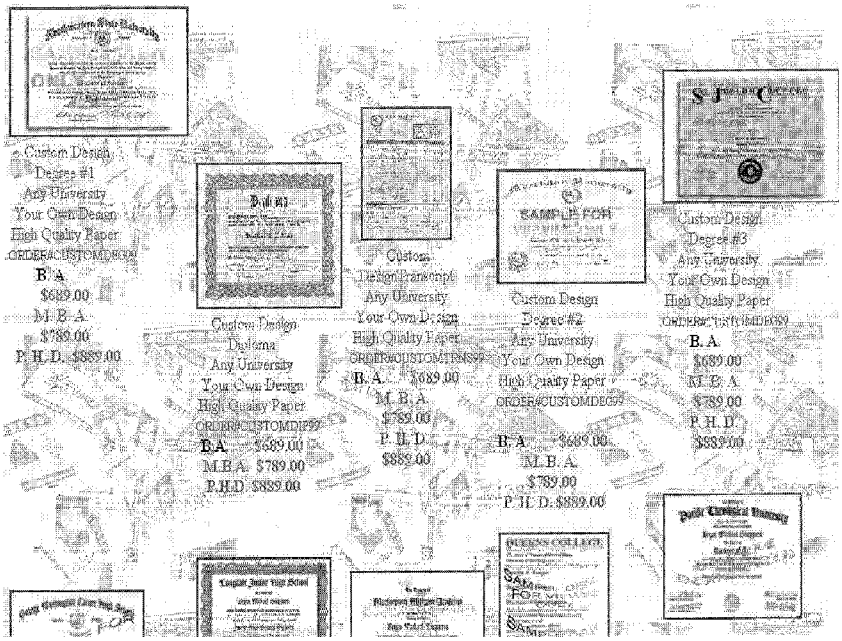
Slide 38



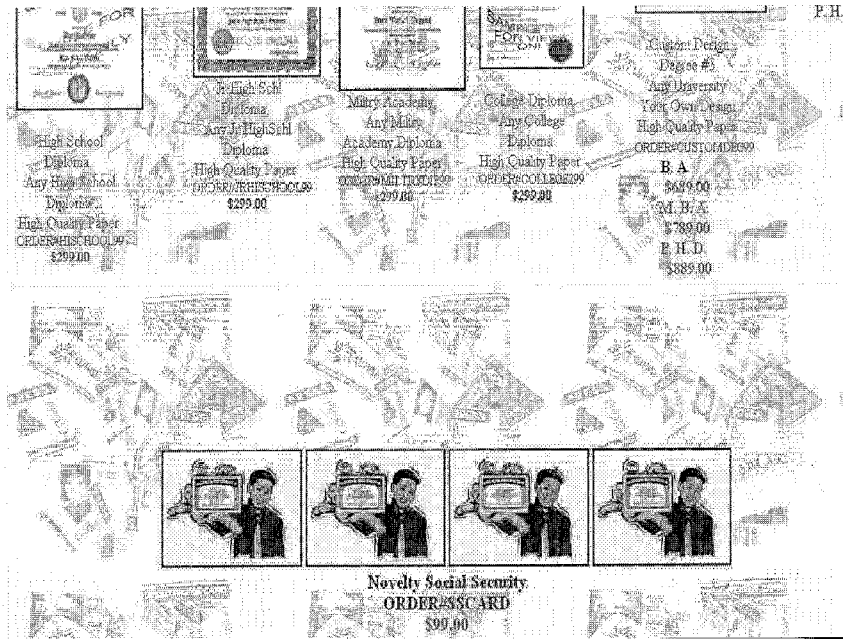
Slide 39



Slide 40



Slide 41



Slide 42

WE ALSO CARRY ANY TYPE OF NOVELTY

MARRIAGE CERTIFICATE	**$189.00**
CUSTOMIZED MARRIAGE	$299.00 (any country)
BAPTISMAL CERTIFICATE	**$189.00**
CUSTOMIZED BAPTISMAL	$299.00 (any country)
DEATH CERTIFICATE	**$189.00**
CUSTOMIZED DEATH CERTIFICATE	$299.00 (any country)
ANY AWARD CERTIFICATE	**$49.00**
CUSTOMIZED AWARD CERTIFICATE	$99.00 (any country)

ANY TYPE OF NOVELTY CERTIFICATE YOU REQUIRE!

Slide 43

NOVELTY
CERTIFICATES/DIPLOMAS/DEGREES
ARE AVAILABLE FROM
ANYWHERE WORLDWIDE

CLICK ON THE CERTIFICATE ABOVE OR REQUEST ONE FROM ANY STATE OR COUNTRY
CUSTOM ORDERS ARE DESIGNED USING THE HIGHEST QUALITY
PAPER AND ALL PRICES REFLECT THE QUALITY OF THE NOVELTY DOCUMENTS WHICH YOU ORDER.

PLACE YOUR ORDER NOW!

Here

CLICK ABOVE TO PRINT OUT YOUR ORDER FORM

ADD A HOLOGRAM OR SEAL TO
ANY NOVELTY ID OR FOR ONLY $44.00
OR A EVEN MORE GENUINE VALID HOLOGRAM SEAL OF AUTHENTICITY FOR $88.00
RAISED AUTHENTIC SEALS FOR CERTIFICATES ONLY $89.00

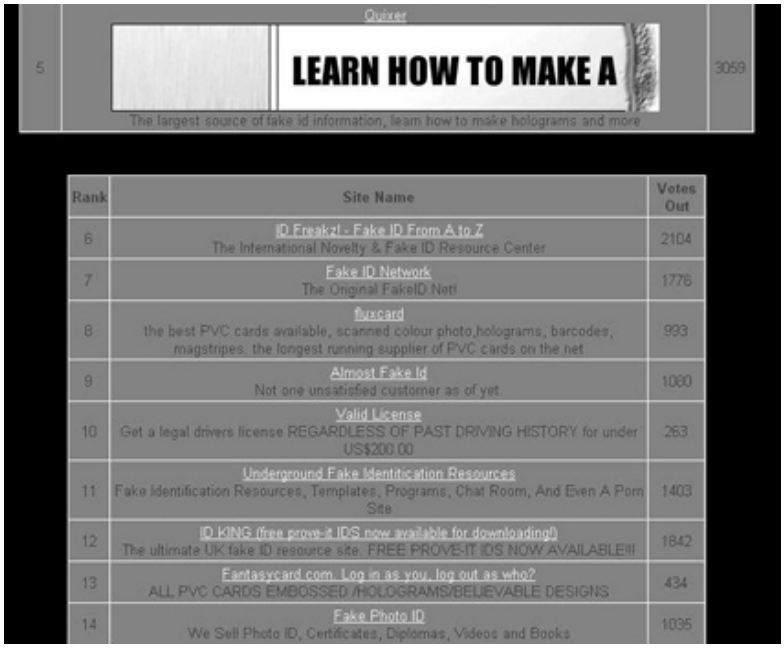
|MAIN PAGE | ID CARD SAMPLES | ORDERFORM|
|F.A.Q. |MOST RECENT ID SAMPLES |MORE ID & DEGREE SAMPLES |

Web Site Designed and updated March 21, 2001
by...P . C . I . S . Design Dept. 2000 & copyright; All Rights Reserved

Slide 44

Slide 45

Slide 46



Slide 47

Slide 48

FakeID REVIEW SITE

Fake ID Review Site

Below you will find the best compilation of honest reviews for Fake ID sites

Some time ago I ordered from several fake ID sites trying to get a decent fake ID to go clubin'. My experience was, to say the least, very disappointing. Either my money was taken, or I was sent something that had no resemblance to the real thing. At that point I chose to create this site and wait to see if there were any good fake ID sites to buy from. Thanks to the outstanding response, I finally got what I was looking for, along with putting together what I feel is a very comprehensive list of both good and bad fake ID suppliers.

Visit our Message Board click here

Post a Message

Website Address	Rating	Location	Processing Time	Reviews
scb-ids.com	Good	Mexico	4 days	This site offers 10 US ID's. All look to be outstanding, custom templates. All reports have been very positive about their ID's. Customers state that the hologrand are flawless, and that the bar codes and magnetic stripes work. This site also allows you to come to their location if you happen to be in Mexico. They even have promo events during spring break. I must report that customers have complained about the shipping time being closer to a week than the 4 days they advertise. If SCB-IDS reads this, you may want to change that. Other than that, all reports lead me to believe that they are a

Slide 49

				good fake ID resource. I have emailed them with general questions and received a prompt response.
photoidcards.com	Ugly	Canada	Not Clear	This site offers everything under the sun. I have had nothing but very negative experiences reported to me from customers. One's that sent cash never received anything. One's that paid by check, waited months, even when paying the outrageous amount for "rush" handling. Their idea of an ID is a kit. You will receive a smaller ID, which you must type in the information. You then glue the picture on and iron on the laminate sleeve they supply. Kinda pathetic. The samples are not designed by them, they are scanned from the bar book. As described above, what you see isn't what you get. No mention on the site of bar codes or magnetic stripe. I have had no reports regarding the diplomas, etc., which they also sell. If their ID's are any indication of their abilities, I would not even give them the chance with their other products. I have emailed them with general questions and received the same generic auto response regardless of the question posed.
fakeidsource.com	Good	Canada	5 Days	This site offers ID's from all US states some college ID's and S/S card. All reports have been extremely positive. They offer correct holograms and working magnetic stripe and/or barcode. A month ago I had several reports that the magnetic stripe was not scanning on the ID's they were sending out. Last week a customer informed me that he sent his ID back in and that it was returned to him "fixed". I emailed the site to ask if the encoding was for real or ES? They assured me that it was a problem with their encoding software and that it has been fixed. Due to this information you may have noticed that my rating has been changed back from 'neutral' to 'good'. I have emailed them with general questions and received a response the same day.
idkurlos.com	Neutral	Canada	Not Clear	This site offers a few US ID's and many other novelty items. I have not heard any experiences from this site, so let me know if you have ordered. The US samples look decent. I cannot see using them for anything as it does not appear that their product would pass the bar book or black light based on design and hologram. Magnetic stripe is not encoded. No mention of bar codes. One thing that concerns me about this site is their proximity to

Slide 50

				photocards. I have emailed them with general questions and received no response. They also have broken links that might indicate they are no longer in business.
members.nbci.com/idfaxus	Ugly	USA	3 days	This site claims to offer US ID's and other types. All reports are that this free-hosted site does not send. I have resisted this site and it is now down. Big surprise. I will not add anymore free-hosted sites. It is the same routine they pop up, scam customers and the site goes down. I have never heard of one that was not a sham on a free host. People who visit this site know better by now to stay away from them.
fakedocuments.com	Neutral	USA	3 weeks	This site offers s/s cards, birth certificates, and ID's. They do not state which ID's, and their samples are very weak. They do not have an address where to send an order and claim that they have run out of paper. This is almost comical. I could not find any mention of security features such as holograms or magnetic stripes on this site. Has anyone ordered from this site? I doubt that anyone has ordered. If you have, please tell me? I will gladly change this review if proven wrong.
diplomas2go.com	Good	USA	2 days	This site offers diplomas, transcripts, and more. I have had nothing but good reports on this site. Customers report that they offer other items not shown on their site such as birth certificates and s/s cards. Apparently you have to email them for those items. I have emailed them with general questions and received answers to all.
novelty-ids.com	Ugly	USA	10-11 days	This site is another one that offers everything under the sun. This site claims that if you are on their site it is because a friend showed you the quality of their product. Every report I have been sent is that the quality they talk about is extremely poor and would never be recommended. That the products they offer would work nowhere for anything with no resemblance to the real thing in any way. They come with no hologram, barcode, etc., just a pure scam. The site does not have any samples for the tons of products offered. This is always a sign of a pure scam. You can only pay by Pay Pal. What people do not realize is that with this form of payment, you have NO recourse for a

Slide 51

				refund from Pay Pal or your credit card company, if you do not like what you receive. They say on their site all sales are final and now you know why.
idfactory.com	Ugly	USA	Not Clear	This site offers a few US ID's and claim to offer others but are "under construction" when I last checked. Every report is that they do not send you anything unless you order COD. When looking at the site I noticed the Georgia ID was scanned from the bar book. A warning sign of a sham. Never order from a site that does not show their own work. They do offer to sell a concealed weapons badge. When I saw this I had to laugh. US states issue permits and not badges for concealed weapons. The one thing that seemed to trick people that emailed me was that they offer COD. What most people do not know is that when you order COD, the deliveryman will not give you the package before you pay the money due. So, this site sends your order, you pay the carrier, you open it to find a pathetic paper card. After you are through screaming, you run after the carrier only to be told "too bad, you have taken delivery and you are stuck".

PLEASE, after surfing around, click my sponsor's banner. It is the only way that I can keep this site going. I would like to note for the ID suppliers that have a h
can step with the emails. Also, I do NOT own or operate any site other than this review site or take payment from ANYONE for my reviews. They are based SOL
proven to me the quality of the items they have received. A "good" or "ugly" review is not given until I have had numerous matching reports and proof of real co
from the same locations twice.

If you have had good or bad experience with a site not listed above, or a different experience than my reviews reflect, please email me. I welcome all questi

Slide 52

Slide 53

Slide 54

Slide 55

Slide 56

California - Berkeley - Chico State - Long Beach State - Pepperdine-
Stanford - USC - UCSB - UCSD
Colorado - Colorado State, University of Colorado
Connecticut - Yale - University of Connecticut
Delaware - University of Delaware
Florida - Florida State - University of Florida - University of Miami
Georgia - University of Georgia - Georgia State
Hawaii - University of Hawaii
Idaho - Boise State
Illinois - DePaul - Northwestern
Indiana - Ball State - Indiana State - Notre Dame - Purdue - University of Indiana
Iowa - Iowa State - University of Iowa
Kansas - Kansas State - University of Kansas - Witchita State
Kentucky - Murray State - University of Kentucky
Louisiana - LSU - Tulane - Xavier
Maine - University of Maine
Maryland - Coppin State - University of Maryland
Massachusetts - Boston College - Holy Cross - University of Massachusetts

Slide 57

Michigan - MSU - University of Michigan - Western Michigan

Minnesota - Minnesota State - University of Minnesota

Mississippi - Mississippi State - University of Mississippi

Missouri - Southwest Missouri State - University of Missouri

Montana - Montana State - University of Montana

Nebraska - Creighton - University of Nebraska

Nevada - UNLV

New Hampshire - Dartmouth

New Jersey - Princeton - Rutgers - Seton Hall

New Mexico - New Mexico State - University of New Mexico

New York - Columbia - Cornell - Hofstra - NYU - St. John's

North Carolina - Duke - North Carolina State - University of North Carolina - Wake Forest

North Dakota - North Dakota State - University of North Dakota

Ohio - Akron - Cincinnati - Dayton - Ohio State - Toledo - Xavier

Oklahoma - Oklahoma State - University of Oklahoma - University of Tulsa

Oregon - Oregon State - University of Oregon

Pennsylvania - Drexel - Duquesne - Penn State - Temple - Penn - Villanova

Slide 58

Rhode Island - Brown - Providence - University of Rhode Island

South Carolina - Clemson - South Carolina State - University of South Carolina

South Dakota - South Dakota State - University of South Dakota

Tennessee - Tennessee State - University of Tennessee - Vanderbilt

Texas - Baylor - Rice - SMU - Texas A&M - TCU - Texas Tech - University of Texas

Utah - BYU - University of Utah - Utah State

Vermont - University of Vermont

Virginia - George Mason - James Madison - Old Dominion - University of Virginia - Virginia Tech - William and Mary

Washington - Gonzaga - University of Washington - Washington State

Washington DC - Georgetown

West Virginia - Marshall - West Virginia State - West Virginia University

Wisconsin - Marquette - University of Wisconsin

Wyoming - University of Wyoming

Slide 59

FakeIDSource.com We offer EXACT novelty ID licenses

Main | Faqs | Order | Contact

The very BEST on the Internet

This is our order form. Print this page, complete all the fields, and mail to the address provided below along with your payment in cash, personal check, money order, "International" Postal money order, or Cashier's Check made payable to VINIR IMAGES. All prices are in US Funds. Please ensure that you have read and understand our ordering information on the "FAQs" page. Thank you for your order!

Print friendly version

The following is for information specific to your novelty ID:

Please fill in one: Novelty ID licenses the State ordered _____

Novelty College ID ordered _____ S/S Card (please circle)

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Height: _____ Weight: _____ Eye Color: _____ Hair Color: _____

Sex: _____ DOB: _____ Organ Donor: _____

Exam Date: _____ Exp. Date: _____ Class: _____

D/L#: _____

Slide 60

S/S#: _____

Additional information specific to your State: _____

X (your signature goes here)

Below must be completed in full by the person ordering the novelty ID card:

Shipping information (keep it legible):

Name: _____

Address: _____

City: _____ State: _____

Zip: _____ Email address: _____

X: _____

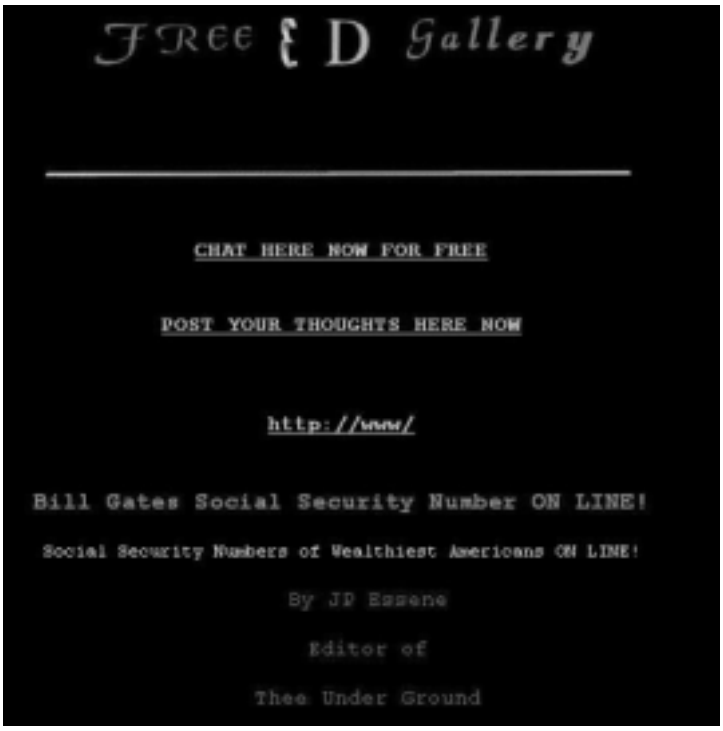
By signing above, I have read and agree to the following terms and conditions: I am ordering a novelty ID card that is NOT a government issued document and not valid in any state or province. I am at least 18 years of age. I will not hold VINIR IMAGES, its employees, ISP provider, or any entity connected to VINIR IMAGES liable for it's misuse. I understand that the novelty ID card I am ordering is very realistic and I will assume any liability attached to it.

Send orders to:
VINIR IMAGES
2135 des Laurentides Blvd. Suite A5
Laval, Quebec H7M4M2 Canada

Slide 61

Slide 62

Slide 63


FREE { D Gallery
CHAT HERE NOW FOR FREE
POST YOUR THOUGHTS HERE NOW
http://www/
Bill Gates Social Security Number ON LINE!
Social Security Numbers of Wealthiest Americans ON LINE!
By JP Essene
Editor of
Thee Under Ground

Slide 64

William H. Gates III XXX-XX-XXXX Worlds Richest Man CEO of Microsoft

Warren E. Buffett XXX-XX-XXXX One of the richest men in the world next to Gates

Paul G. Allen XXX-XX-XXXX Another BILLIONAIRE from Microsoft

Gordon Earle Moore XXX-XX-XXXX Of INTEL fame

JOHN W. ELDGE XXX-XX-XXXX Can you say MEDIA TYCOON

Jim C. Walton XXX-XX-XXXX Walmart Heir

Helen R. Walton XXX-XX-XXXX Walmart Heir

Alice L. Walton XXX-XX-XXXX Walmart Heir

John T. Walton XXX-XX-XXXX Walmart Heir

S. Robson Walton XXX-XX-XXXX Walmart Heir

Walter H. Annenberg XXX-XX-XXXX Philadelphian's Richest

Norman N. Waitt, Jr. XXX-XX-XXXX Gateway Computers

Arthur Ochs Sulzberger XXX-XX-XXXX- Publisher NY TIMES

Gen. Colin L. Powell XXX-XX-XXXX - Famed GULF WAR Colonel and possible FUTURE PRESIDENTIAL CANIDATE

R.E. Turner XXX-XX-XXXX - Jane Fonda's husband TURNER MEDIA TYCOON

Slide 65

JP Essene

Editor

Thee Under Ground

LOTR

E Mail J.P. Essene

DID YOU KNOW

In 1997 the mystic named Rollog wrote the 902 Prophecy. The 902 Prophecy was posted to various Usenet groups and has been mentioned 1,000's of times since many future events have recently connected to it.

An event predicted in the 902 Prophecy was Swissair 111.

Slide 66

Sollog who claims the ability to predict plane crashes, such as TWA 800 actually put the date, flight number, departing city and even the death count of flight 111 in that Prophecy.

The Clinton scandal was in the prophecy as well. He also predicted the dates of 4 major acts of terrorism including the Ireland August 15th bombing and the US Embassy bombings They all occurred on dates given in the 902 Prophecy.

Sollog says his gift of fore telling the future so accurately is due to his warning about Nukes. He says mankind is on the threshold of Nuke Terrorism. If you would like to spread Sollog's WARNING about NUKES, by donating monies to fund a large mainstream media purchase email me.

These are some of Famous Prophetic hits of the Prophet Sollog

TWA 800

Diana's Death

OK City Bombing

Mexicali Quake

Rabin's Assassination

Mike Kennedy's death

Embassy Bombing

New Guinea Tidal Wave

Slide 67

If you want to read more about Sollog, these are the best sources.

Sollog Message Board

Over 50 Sollog articles.

Sollog's Site

CHAT here about Sollog

More Feature Articles by JP Essene

FEA tures

Editorials by JP Essene

EDI torial

Slide 68

Slide 69

Slide 70

Slide 71

Slide 72

Slide 73

Social Security Administration

OFFICE of the INSPECTOR GENERAL

Internet Web References

www.attbusiness.net
www.dogpile.com
www.ussearchit.com
www.unlisted-etcetera.com
www.photoidcards.com
www.top10id.cjb.net
www.fakeidsite.com
www.fakeidsource.com
www.theeunderground.com
www.nextcard.com

Chairman SHAW. Thank you, Mr. Robinson. Mr. Fabozzi.

STATEMENT OF MICHAEL FABOZZI, DETECTIVE, COMPUTER INVESTIGATIONS AND TECHNOLOGY UNIT, SPECIAL INVESTIGATIONS DIVISION, NEW YORK CITY POLICE DEPARTMENT, ACCOMPANIED BY JAMES DOYLE, SERGEANT

Mr. FABOZZI. Good morning, Mr. Chairman and members of the Subcommittee. On behalf of Mayor Rudolph Giuliani and Police Commissioner Bernard Kerik, we would like to thank you for the opportunity to appear before you today to discuss this very important subject.

My name is Detective Michael Fabozzi. Seated next to me is Sergeant James Doyle. We share a combined 36 years experience in the New York City Police Department (NYPD). During that time we have patrolled the New York City subways, housing developments and ultimately went on to serve in the NYPD's Detective Bureau. Presently, we are assigned to the Computer Investigation and Technology Unit, which is part of the Special Investigations Division. Investigators in the Special Investigations Division are responsible for the investigation of white collar crimes, specifically bank and brokerage fraud, credit card fraud and identity theft.

For the past several years we have been assigned to the Computer Investigations and Technology Unit, a squad that has been at the forefront in the area of investigating financial crimes perpetrated through the Internet.

Over the past five years there has been a significant increase in crimes where criminals compromise personal identifying data of victims in order to commit identity theft. The information that falls into criminal hands includes such information as name, date of birth, Social Security number, banking account number and other personal and financial information.

Victims of identity theft, like other crime victims, may feel personally violated. This is especially true in light of the vicious cycle of events that typically follows the occurrence of this crime. Imagine for a moment a recently married couple just starting out their life together. They work hard and save enough money to make a down payment on their first new home only to be denied a mortgage because of a negative payment history, information they knew nothing about. The trouble of rebuilding personal credit may be a more horrifying experience than the illegal charges on a credit card statement. The trauma that this type of fraud causes innocent victims is unimaginable. Moreover, once the crime is discovered and reported, victims are left to fend for themselves in attempting to clear their credit history and good name.

Our unit has successfully conducted numerous investigations where criminals have used the personal information not only to obtain credit cards and personal loans but also to purchase cars and homes. We have seen defendants who stole the identity of others create phony identification on common computer peripherals, such as scanners and printers, and walk into banks and walk out with the accountholder's money. One was even arrested using the name, date of birth and Social Security number of her victim. Although

we in law enforcement garner some sense of satisfaction when we make arrests for these crimes, it is not enough when compared to the amount of time and energy a victim spends trying to undo the work of these criminals.

Recently, I was the arresting officer and lead investigator of a team of NYPD detectives, postal inspectors and Secret Service agents in the Abraham Abdallah case, a case that received national and international exposure. Since it is still an on-going investigation, my comments are limited only to the information that has been reported publicly.

Abraham Abdallah, a busboy in a local restaurant in Brooklyn, New York, was able to successfully obtain the personal information, such as date of birth, name, Social Security number, phone and address and sometimes the bank and brokerage information by using the Internet and other sources. Working as a busboy, Abdallah allegedly stole credit card numbers of various customers and then used those credit card numbers to order and purchase merchandise over the Internet.

In addition to ordering merchandise with stolen credit cards, he used the personal information of his victims to open up new credit card accounts. He requested that new cards be mailed to a new address, usually a mail drop. A mail drop is a P.O. box or mail receiving agency that receives mail for an individual, such as Mailboxes, Etc. New credit card accounts were then opened at these mailbox drops in the name of celebrities and many prominent, well known business leaders. Using these new credit card accounts, Abdallah allegedly went into the local library where he was able to purchase credit history reports on line.

Through the use of on-line information providers and other Internet-based databases, Abdallah was able to penetrate the banking and brokerage accounts of his victims using a common trick called social engineering. Social engineering is the process whereby an individual misleads another, such as a customer service rep, into providing personal information about an individual or an account. Once Abdallah obtained the personal account information and perhaps a password, he was then able to steal a vast amount of money from the accounts of our nation's wealthiest individuals.

This tale of the busboy cyber-thief is a frightening testament to the vulnerability of the entire e-commerce system, a system that has successfully lulled America into believing that encryption and on-line privacy policies have made internet transactions secure. The holes in our system are everywhere—at restaurants, department stores, merchant counters, doctors' offices, insiders at banks and brokerages and HMOs to the nation's three credit-reporting bureaus. By finding just a few holes, Abdallah allegedly was on his way to stealing millions of dollars.

We urge this Committee to take the necessary steps to develop new ways to prevent this type of fraud without sacrificing the privacy rights of the consumers. Specifically our legislative recommendations are as follows.

Entities which have access to consumers' personal identifying information should be strictly accountable as to who they provide such information to and the purpose that the information is being provided for.

Credit reporting agencies should have to notify consumers when inquiries regarding credit histories are made. The consumer should have the ultimate ability to deny such information from being disseminated by the credit reporting agency.

Internet service providers and web sites should be mandated to maintain detailed records of their transactions. Unlike telephone companies that keep detailed records of calls which are of great value to law enforcement in its investigation of identity theft, Internet companies have no set standards as to what records of transactions are kept, thereby providing an impediment to investigating identity theft.

The posting of Social Security numbers on the Internet should be strictly prohibited.

We believe that some of these legislative safeguards, if enacted, can have a significant impact on the crime of identity theft. Thank you for the opportunity to address the Subcommittee.

[The prepared statement of Mr. Fabozzi follows:]

Statement of Michael Fabozzi, Detective, Computer Investigations and Technology Unit, Special Investigations Division, New York City Police Department

Good Morning, Mr. Chairman and members of the Subcommittee. On behalf of Mayor Rudolph Giuliani and Police Commissioner Bernard Kerik, we would like to thank you for the opportunity to appear before you today to discuss this very important subject.

My name is Detective Michael Fabozzi. Seated next to me is Sergeant James Doyle. We share a combined 36 years experience in the New York City Police Department. During that time we have patrolled New York City's subways, housing developments and ultimately went on to serve in the NYPD's Detective Bureau. Presently, we are assigned to the Computer Investigations and Technology Unit, which is part of the Special Investigations Division. Investigators in the Special Investigations Division are responsible for the investigation of white-collar crimes, specifically bank and brokerage fraud, credit card fraud, and identity theft. For the past several years, we have been assigned to the Computer Investigations and Technology Unit that has been at the forefront in the area of investigating financial crimes perpetrated through the Internet.

Over the past five years, there has been a significant increase in crimes where criminals compromise personal identification data of victims, in order to commit identity theft. The information that falls into criminal hands includes name, date of birth, Social Security Number, banking account number, and other personal and financial information.

Victims of identity theft, like other crime victims, are made to feel personally violated. This is especially true in light of the vicious cycle of events that typically follows the perpetration of this crime. Imagine for a moment, a recently married couple just starting out in their life together. They work hard and save enough money to make a down payment on their first new home only to be denied a mortgage because of a negative payment history reflected in a credit report—information that they knew nothing about. The trauma this type of fraud causes its innocent victims is unimaginable. Moreover, once the crime is discovered and reported, victims are left to fend for themselves in attempting to clear their credit history and good name.

Our unit has successfully conducted numerous investigations where perpetrators have used the personal information to not only obtain credit cards and personal loans, but also to purchase cars and homes. Although we in law enforcement garner some sense of satisfaction when we make arrests for these crimes, it is not enough when compared to the amount of time and energy a victim spends trying to undo the work of these criminals.

Recently, I was the arresting officer and I am the lead investigator in the Abraham Abdallah case—an investigation that received national and international exposure. Since the matter is still an ongoing investigation, my comments are limited to only that information that has been reported publicly. Abraham Abdallah, a busboy in a local restaurant in Brooklyn, New York was able to successfully obtain personal information such as names, dates of birth, social security numbers, phone numbers, and sometimes bank and brokerage account information by using the

Internet and other sources. While working as a busboy, Abdallah stole credit card numbers of various customers and then used those credit cards to order and purchase a variety of items over the Internet.

In addition to ordering merchandise with stolen credit cards, he used the personal identification information of his victims to open up new credit card accounts. He requested that the new cards be mailed to a new address—usually a "mail drop." A mail drop is a P.O. Box or Mail Receiving Agency that receives mail for an individual, such as Mailboxes Etc. New credit card accounts were then opened using these mailbox drops as the address of individuals, including celebrities and even a few prominent, well-known business leaders. Using these new credit card accounts, Abdallah went to the local library where he was able to purchase credit history reports on-line.

Through the use of on-line information providers and other Internet based databases, Abdallah was able to penetrate the banking and brokerage accounts of his victims by using a common trick called "social engineering." Social Engineering is the process whereby an individual misleads another person such as a customer service representative into providing personal information about an individual or account. Once he obtained the account information and perhaps an account's password, he was then able to steal a vast amount of money from the accounts of our nation's wealthiest individuals.

This tale of the busboy cyber thief is a frightening testament to the vulnerability of the entire e-commerce system—a system that has successfully lulled America into believing that encryption and on-line privacy policies have made Internet transactions secure. The holes in our system are everywhere—at restaurants, department stores, merchant counters, doctor's offices, insiders at banks and brokerages, places of employment and at the nation's three major credit reporting bureaus. By finding just a few of holes in the system, Abdallah was on his way to stealing $100 million.

We urge this Committee to take the necessary steps to develop new ways to prevent this type of fraud without sacrificing the privacy rights of the consumers. Specifically, our legislative recommendations are as follows:

- Entities that have access to a consumer's personal identifying information should be strictly accountable as to who they provide such information to and the purpose that the information is being provided.
- Credit reporting agencies should have to notify consumers when inquiries regarding credit histories are made. The consumer should have the ultimate ability to deny such information from being disseminated by the credit-reporting agency.
- Internet service providers and web sites should be mandated to maintain detailed records of their transactions. (Unlike telephone companies that keep detailed records of calls that are invaluable to law enforcement, Internet companies have no set standards as to what records of transactions are kept, thereby providing an impediment to investigating identity theft.)
- The posting of social security numbers on the Internet should be prohibited.

We believe that some of these legislative safeguards, if enacted, can have a significant impact on the crime of identity theft. Thank you for the opportunity to address the subcommittee. We will be happy to answer any questions that you may have.

Chairman SHAW. Thank you. Mr. Collins? Mr. Becerra?

Mr. BECERRA. Thank you, Mr. Chairman. And thank you to all the witnesses for their testimony.

Let me begin by asking Mr. Huse his thoughts on a couple of things. One, we know that the use of the number, the Social Security number, is widespread and we know that in many cases private, including public sector agencies and firms, rely on the card to conduct business. We will hear in the next panel many witnesses who will tell us that we are going too far or that there are things that we could do to curtail the misuse of the number but still allow it to be used for other purposes. Some people say that we have been able to track down missing children, we have been able to track down deadbeat fathers by using the Social Security number.

Is there a way, in your opinion, of addressing the concern of identity theft and, at the same time, trying to address the concerns raised by the private sector most particularly in the use of the card to undertake activities which are legitimate and could be beneficial to the public?

Mr. HUSE. I believe there is. We have to accept that the Social Security number is the de facto national identifier and its uses, both by the governmental entities at all levels and the private sector is too imbedded for us to change. It is probably impossible to change it.

But, I think if we regulate an attempt to control the movement of these identifiers in terms of the sale and use of credit histories and credit information and make the entities that do this accountable for the sale and use of these by obtaining the permission of the cardholder himself or herself or notification at the very least, we have gone a long way in slowing down the reckless movement of these numbers, which is at the base of a lot of the criminal problems you have heard about this morning.

I think the bill that the Committee put together last year, H.R. 4857, struck the right compromise there between balancing out all of the interests, leaving something for commerce, leaving something for government but, at the same time, giving people the right to have their good name intact.

Mr. BECERRA. Thank you.

Let me ask any of the folks in law enforcement if they can give us some thoughts on how we can also try to curtail the activity that we see through this presentation that you made, Agent Robinson, where, in effect, you are promoting the use of fraudulent cards, identity cards, and you are, in essence, giving people license to go out there and commit fraud.

Is there any way for us to try to strike at the type of businesses that would market this type of product yet still allow what Mr. Huse identified as legitimate interests to continue within the private and public sectors in the use of, say, the Social Security number?

Mr. ROBINSON. Most of the sites that we actually visited and the companies that are selling these Social Security cards are usually not selling them for legitimate purposes and that, to me, gives us that feeling that as soon as you can see the card and see the fact that the novelty sticker or the sample sticker can be actually pulled off the card and usually they try to protect themselves with a disclaimer but most of the individuals or the individuals who will purchase those cards, I do not think there is a legitimate reason for selling a Social Security card over the Internet or anywhere else.

Mr. BECERRA. So, is there a way to go after that type of enterprise that really does not have a legitimate purpose, other than to help someone commit identity fraud?

Mr. HUSE. I think the accountability that we seek for these entities, to make them responsible for what they traffic in with both criminal sanctions and civil money penalty sanctions, these are the ways to push them back from these enterprises.

Mr. BECERRA. So you would make them criminally liable if someone, for example, is apprehended after using a fake ID obtained by one of these Internet sites, that that Internet company would be

equally responsible, criminally liable in that case of any offense that may have been committed by the individual who obtained the fake ID?

Mr. HUSE. That is correct.

Mr. BECERRA. Thank you. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Johnson? Mr. Pomeroy?

Mr. POMEROY. I want to thank the entire panel. This has been extremely interesting. I regret the inconvenience and disruption to especially our witnesses that have been defrauded.

Inspector General, on this point of how do we deal with this in a reasonable way, I would like to follow my colleague's questions.

Presently in the implementation of Gramm-Leach-Bliley legislation there have been millions and millions of consumer privacy notices mailed out. I know a number of individuals, your basic average—a couple of retirement accounts, bank accounts, what have you—will have gotten a half dozen notices and I am not sure we have exactly clarified in the public's mind precisely the kind of informed status we wanted to achieve relative to privacy generally.

Are suggestions, in terms of how to deal with this problem, would they require additional notices I am afraid potentially confusing the public in terms of the status of all this?

Mr. HUSE. I think the public is fairly well informed about the fact that this is a problem. The identity fraud problem, I think just even in recent months, you cannot turn on the television at night and not get an identity fraud story on one of the local television stations. In fact, I think one of them in the Baltimore area broadcasted a story very similar to Agent Robinson's demonstration here today last night.

If we stick to trying to regulate what we can or to control what we can, I think the public will accept this, that they have a right, we all have a right to know to what uses our Social Security account number is being put to and when that information migrates from one database to another we should be notified as to the intent or purpose. I think that is a reasonable expectation for all of us.

It will add costs to some of the financial uses of the SSN but I think that is a far better route to take than to try to expunge the use of them entirely because I do not think we could do that.

Mr. POMEROY. I was in the State legislature when we allowed the Social Security number to be substituted for driver's license and the public liked it. They did not have to remember their driver's license number anymore; it was simple. They had the opportunity under our law to choose either one but overwhelmingly there was a preference, just for simplicity's sake, to do that and that was pre having all these PIN numbers that you now have to remember in order to access your various accounts.

There are two sides to the coin. I am very concerned about the public security issue you present so well on abuse of the Social Security number but, on the other hand, there is a convenience of business issue that I am trying to not totally interfere with, either.

Mr. HUSE. We all recognize with this rush of technology and the change that it has made in our lives just in the last 20 years that ultimately the solution to all of this will be some other kind of national identifier. I mean that will come in time. What form that takes, whether it is a biometric thumbprint or eye scan or what-

ever, that will happen inevitably. Then the pressure on the Social Security number will go away. But to go from where we are today to there, no one can estimate when that will happen. Those biometrics exist now but they are too costly.

So, I think we have to be careful here that we keep this balance. I think the way 4857 is put together, it has some measures that give us an opportunity to make some demonstrable effort in terms of trying to protect the privacy of people's identification data and yet, at the same time, still allowing enough commercial and governmental use of the number to keep commerce going.

Mr. POMEROY. Do you have any ideas about how we might easily assist victims in terms of getting everything straightened around, some central registry they could go to where in a one-call way they have their issues dealt with, as opposed to the incredible burden we place on victims today?

Mr. HUSE. Well, the Congress has made a lot of effort that way in the last five years and de facto, that kind of exists now between the Federal Trade Commission's hotline and the Social Security Administration's Office of Inspector General (OIG) hotline, who completely cooperate with each other. They have become really, in many instances, the court of last resort for a lot of victims of financial crime.

What we need to do a better job in is putting together all of the pieces of law enforcement at the local, county, state and Federal levels to work on these things. Again the bill addresses some of this with the ability for my office, for example, to be able to task force with all of these law enforcement entities to create the kind of synergy we need to do a better job with this because we hear the victims speak about the inability of a lot of law enforcement to really make an impact.

You see, this is a crime that you need real-time information for at the time of an apprehension and when that does not exist, that is how these people survive and move on and metamorphose into something else the next day with more stolen IDs.

Mr. POMEROY. Thank you.

Chairman SHAW. Mr. Collins?

Mr. COLLINS. Thank you, Mr. Chairman.

I have a question for Agent Robinson. On the website Dog pile you have instant Social Security number searches. Can you just type in a number there and hit fetch and it will go and gather that information?

Mr. ROBINSON. Yes, sir. What I actually used was the search engine and wrote in the quote to go out and search for websites that would actually assist me in obtaining instant Social Security number searches. No actual number was placed in there.

Mr. COLLINS. Okay, that just searches for websites, then.

Mr. ROBINSON. Correct.

Mr. COLLINS. On any of the websites could you just put in a number and it would search that number?

Mr. ROBINSON. With the Social Security number, if I had the Social Security number?

Mr. COLLINS. Just make up a number.

Mr. ROBINSON. No, you could put in someone's actual Social Security number and at those various websites they could go out and

verify it for you or you could actually request a Social Security number that matches the information that you are providing to the service, such as the name, date of birth and the current address of an individual, is usually the minimum that most of those sites would need.

Mr. COLLINS. But if I had none of that information, I just made up a Social Security number and asked it to search that, would it search it?

Mr. ROBINSON. Some of those sites will do that and will provide that service. If you provide them with a Social Security number I think it is the second site that we used, the Et cetera site would provide that service. You actually place in the Social Security number and it will give you a response and in some of those responses—it varies—some responses will be just the name and some responses will be the name and the address. The response varies based on the price that you pay.

Mr. COLLINS. It has been mentioned holding these people accountable that provide this type of information. If they are not a U.S. entity or using the net from another country, how do we approach that, that accountability question?

Mr. ROBINSON. Well, the law enforcement agencies here will have to work closely with those countries that have those various websites that offer that service and we would have to see what their laws are in that particular country. Usually, regardless of what the laws are in that particular country, the person is going to misuse the information here in the States.

Mr. COLLINS. Okay. This thing becomes a real mountain as you start moving it, does it not?

Mr. ROBINSON. It does.

Mr. JOHNSON OF TEXAS. Would the gentleman yield?

Mr. COLLINS. I would be glad to, Mr. Johnson.

Mr. JOHNSON OF TEXAS. Following up on that question, if some country like Russia, for example, had somebody in there manipulating our system and providing fraudulent information and we do not have any arrangement with them, I bet, between law enforcement to take care of that problem, how do we address that?

Mr. HUSE. Actually, the Department of Justice and the Department of Treasury both have foreign operations in most of these countries now. In fact, my own son is one of the agents from the Secret Service that oversees doing this, teaching financial crimes investigations to these new former Soviet republics and countries where they do not know much about financial crime.

Mr. JOHNSON OF TEXAS. But they know how to mess with the Internet.

Mr. HUSE. And they are, but we actually have on-going efforts to bring up law enforcement in these countries to a level of cooperation that we have on other types of crime now through Interpol and other——

Mr. JOHNSON OF TEXAS. Have you run into any of that with other countries trying to manipulate our system?

Mr. HUSE. The NYPD, I am sure, can answer that better than we can.

Mr. FABOZZI. We have done investigations and what we do in the Computer Crime Squad is that we find where the host is, the com-

puter where it is located that is actually hosting the site of the ID fraud or the novelty ID card, Social Security cards, and the host computer may be in the Soviet Union and that ends our investigation. We forward that to Interpol or another Federal agency.

Mr. JOHNSON OF TEXAS. Have you ever had any indication that the Chinese might be doing that?

Mr. FABOZZI. Not at this time.

Mr. JOHNSON OF TEXAS. Okay, thank you.

Chairman SHAW. Mr. Ryan?

Mr. RYAN. Thank you, Mr. Chairman.

Mr. Huse, I would like to ask you a couple of questions. You testified that legislation is needed to stop the ready availability of Social Security numbers over the Internet. I know we have been talking about last year's bill, 4857. Is there something else that you think is needed in this bill or are you pleased with the product from your perspective that came out of last year's Committee?

Mr. HUSE. I am very pleased with the product that came out last year. I think if we can get that, we are a long way to where we have to go.

Mr. RYAN. You also mentioned that you have a hotline up and running that you have had for several years. Have you noticed a marked increase in allegations involving identity theft and Social Security misuse?

Mr. HUSE. Well, each year since we have had the hotline up and running we have received more and more allegations. A little over half the allegations we receive have to do with Social Security number misuse and identity fraud and those have increased every single year.

Mr. RYAN. And that is in a steep incline?

Mr. HUSE. It is going up. It is going up.

Mr. RYAN. Also you stated that your office has conducted undercover operations where you have purchased actual counterfeit Social Security number cards. You state that you are currently involved in an investigation of an Internet auction company that is selling names and Social Security numbers. Can you tell me about how many individuals or different companies are in existence today that do this?

Mr. HUSE. We do not have exact figures. I do not think anybody does. They crop up like mushrooms overnight on your lawn.

Mr. RYAN. Pretty simple to get started?

Mr. HUSE. It is very simple to start a business on the Internet but we do not have exact figures.

Mr. RYAN. I wanted to ask the two officers, Detective Fabozzi and Detective Doyle, all of our Social Security numbers are out there. Nothing can be done immediately to protect against that. But what would you recommend to individuals and citizens that they can do to protect their identity at this time right now? Even if they take such steps, what are the chances we can stem identity theft aside from any type of legislation that would be passed?

Mr. DOYLE. The biggest thing would be awareness of how prevalent your number is out there and your Social Security number is the key that unlocks the ability to do a lot of this identity-type fraud.

The biggest problem we see with our victims is that helplessness when they discover they are a victim, how they have to try to repair their own credit. We try to make them aware of the FTC's website that has a lot of very good steps on how to repair their credit. All the phone numbers are on one website to make these fraud alerts, to get the credit-reporting agencies to put that alert on their accounts so that they are notified when a new account is opened up. But unfortunately, they are the last ones to know when these accounts are opened up because the bad guys are opening up good accounts using their good name so the accounts are going to be good until they run them into the ground.

So again people have to keep in mind their own credit reports, as Ms. Robinson pointed out. She looks at it every year. But from year to year, that is plenty of time for someone to run up credit report——

Mr. RYAN. So at this time it is really just reactive, is it not?

Mr. DOYLE. Yes, it is.

Mr. RYAN. Nothing one can really do proactively to prevent this from occurring.

Mr. FABOZZI. Proactively, one thing you can do is run your credit report annually, if not more. Second, be diligent as far as checking any bills that you receive in the mail and destroying them, shredding the bills and account numbers, name, address. I would not send mail out, like bills going out to different companies, in your mailbox. I would actually mail them myself at the post office because if you left them out with the flag up in front of your house, someone could come by and just take the mail out of your box and then they have your check number which has your banking information, maybe an account number, Social Security number.

Mr. RYAN. That is very interesting. Thank you. I yield, Mr. Chairman.

Chairman SHAW. Thank you.

In looking through the book that you all supplied to us there are some incredible things that can be bought—death certificates, marriage licenses. Now who wants more than one marriage license? I have no idea. But driver's license?

Do these documents appear to be accurate? If you are stopped by a policeman for a speeding violation in Florida and you have a fake Florida ID will you fool the Florida Highway Patrol?

Mr. DOYLE. Michael also had another case where this one group of individuals had very real-looking New York State driver's licenses including the magnetic code on the back and he will talk more about it.

Mr. FABOZZI. What they were able to do is first of all, create the magnetic stripe on the back of the driver's license. In New York State it has a high amount of security features in it, such as the color and the security features that are built into the United States currency. But what they were able to do is through using pickpockets and burglars and working in a group they actually stole the identity, meaning they stole the driver's license and then using computers they created a new driver's license using the exact number of the victim but substituting the photograph.

So let us say I would steal Sergeant Doyle's identification. I would put my picture on his driver's license but all the other infor-

mation—account number, date of birth, address—is valid. So if they were stopped by police and I produced this license and even if the officer ran the driver's license through his computer, the number of the license would be valid and it would come back as James Doyle but it would just have my face on it.

Chairman SHAW. But his description. What if you are 6 foot and 3 inches and he is 5 foot and 4 inches? Would that come through like that?

Mr. FABOZZI. I am sorry, Mr. Chairman. I did not hear you.

Chairman SHAW. What if there was a great difference in your height and weight, description, color of hair, color of eyes, those types of things that are on a driver's license?

Mr. FABOZZI. That would be diligent upon the officer that pulled him over. Also, since it is a counterfeit document, you can alter that on the phony one but the records would come up legit on the print-out.

Chairman SHAW. I see that there are college diplomas. Are not some of these things now illegal? Is not issuing someone a driver's license illegal now?

Mr. FABOZZI. Yes. In New York State it is a forged document so if you are using it, let us say, to impersonate someone or even just to get a driver's license, it is possession of a forged instrument, which is a felony in New York State.

Chairman SHAW. Is it a felony to distribute these documents?

Mr. HUSE. They distribute them as novelty items.

Mr. FABOZZI. They skirt the issue by putting in a banner that this is for novelty purposes only.

Chairman SHAW. I see they have a marriage license as a novelty item, 180 some dollars. That is a hell of a joke. And college and high school diplomas, I see right here. I think probably other committees should really broaden our net here to see exactly what is going on and universities should be able to be protected and have their name protected under copyright or something so that there is a cause of action that can close these people down.

Mr. HUSE. Mr. Chairman, this has gone on for a long time. What makes it really critical that we act now is that the Internet takes us, because of the speed with the way these things are done, to an entirely different place.

When we just were dealing with paper and counterfeited documents, and trafficking in documents for false IDs has been as long as I have been in law enforcement——

Chairman SHAW. I know the green card has been——

Mr. HUSE. Exactly. The Congress has attempted to keep up with this through the years but what the Internet did or the electronic age is it takes us to an entirely different level of activity where it makes it so easy for people to change identities overnight and it is risk-free. Why would not criminals do this, where they can steal from you or me or anybody else without involving any personal risk?

And it is allowed because there is no way for us to know we have been victimized under the present system.

Chairman SHAW. Well, I think it is illegal to use this type of identification. Now we have to be sure that it is illegal to distribute it.

Mr. HUSE. Right. Our traditional approach has been to attack it after the fact.

Chairman SHAW. We need to go back to the wellhead.

Mr. HUSE. Right.

Chairman SHAW. Miss Robinson, you spoke of the purchase of a car in San Antonio. Did that occur after you alerted the credit-reporting agency of your identity theft or after her arrest? Where is the point in time that that happened? Do you know?

Ms. ROBINSON. Actually, from the beginning I had been in contact with the San Antonio police because when she went into the jewelry store in the San Antonio mall they did contact the police immediately and actually they contacted the police before they contacted me. So they were well aware that this was going on before I even knew about it.

Chairman SHAW. How did they know?

Ms. ROBINSON. Because when she came into the jewelry store on the second day to make purchases they ran my full credit report and noticed that I had a Maryland address, although she had provided a San Antonio address. They contacted their fraud department and they double-checked the information and when they double-checked it—because when she first came in they did an instant credit report and the only thing that came back was a credit score.

The second time she came in the next day, when they thought the activity was suspicious, they ran a full credit report and saw that my last reported address was in Maryland. So they decided that they would contact this Nicole Robinson in Maryland to make sure that it was a different person and because I was a different person, they contacted the San Antonio police. So they were well aware that this was going on.

Chairman SHAW. They went well beyond what most merchants would do. Most merchants would probably just shrug it off. So they are to be complimented. That is wonderful.

Ms. ROBINSON. Yes.

Chairman SHAW. And how about the insurance from GEICO?

Ms. ROBINSON. Well, when I contacted GEICO they agreed the day that I called them to remove my identifying information from this policy. Then they said they would contact her to have her provide a different Social Security number and no longer use mine on the policy.

Chairman SHAW. Mr. Moneme, you indicated there were only two pieces of identity that were stolen from you, credit card and your driver's license that had your Social Security number on it. What State is that?

Mr. MONEME. The State of Ohio.

Chairman SHAW. Are they still using Social Security numbers on driver's licenses?

Mr. MONEME. I believe so.

Chairman SHAW. I know Virginia did for a while but I think they have stopped that practice.

Mr. MONEME. I have a DC driver's license now and I had the option of selecting a unique number and I chose to do so.

Chairman SHAW. Kim just told me that it is optional in Ohio, also, so I assume you allowed them to use that number. Actually,

you think it is a convenience until you start really thinking it through and then you say whoops.

Mr. MONEME. Right, that was my feeling.

Chairman SHAW. Do you feel that without your social security number that all of this would have been avoided, despite the fact that your wallet was stolen?

Mr. MONEME. I feel, sir, that was the only piece of information that had anything unique. On all the applications there were different addresses, there was a signature that did not match up to the one on my driver's license. That was the only piece of information that connected me to that incident.

Chairman SHAW. Mr. Huse——

Mr. HUSE. I just wanted to correct——

Chairman SHAW. You go ahead but then I have another question for you.

Mr. HUSE. Very good. The only thing I wanted to correct, Mr. Chairman, because it proves that we do try to make an effort here and Congress did pass a law last session, the Internet False ID Prevention Act of 2000, which makes it illegal for these novelty ID items to be sold but you can see from real-time today they are still out on the Internet and available. It is illegal to do that but that does not mean it is not done.

So, that piece has been dealt with in terms of the law. It is a criminal act to do that. But with the way the electronic world works, it is not a person. It is just a site and they move and they pop up all the time.

Chairman SHAW. Well, can you elaborate on that? We always hear we are concerned about people introducing viruses that get into computer programs. Is there any way we could backup a virus and blow it up?

Mr. HUSE. They do, but a lot of these are break-out operations that just go on for what they can——

Chairman SHAW. How do you get on the internet and whose service are these on? I mean they have to subscribe to a service somewhere.

Mr. DOYLE. What our unit does, we do a lot of these. If I have a website I want to put up I would just find a company that hosts websites, give them my web page, as you saw——

Chairman SHAW. Is it trackable to——

Mr. DOYLE. They are trackable if the right records are kept.

Chairman SHAW. Is it illegal? If I am one of these contractors that puts people websites up, could I be held criminally responsible for allowing this to go on?

Mr. DOYLE. It depends if you know what is on that website. Sometimes we have web-hosting companies that have no clue what is on their websites. They just have pages that are up-loaded from a remote location.

Chairman SHAW. Well, should we make sure that they have a clue?

Mr. DOYLE. That was one of our recommendations, Mr. Chairman, was to look at better record-keeping by these Internet service providers as to who has this website, where is it hosted? We looked at some websites up there about where these novelty items are being sold from and I can register a website and make it appear

to be somewhere else. It is again the skills of detectives like Mike Fabozzi that you may be able to trace back where is that website hosted and maybe conduct an investigation into buying these items in an undercover capacity, say, and trying to find out the money trail.

But tracing these things back, again the skill of law enforcement has to get up to speed. Again there are very few detectives that could do what Mike does to find where is that website hosted, who is responsible for it. The records sometimes are not there.

Chairman SHAW. Mr. Huse.

Mr. HUSE. I think in my written testimony I mention an eBay case where someone was auctioning Social Security numbers. When we contacted eBay about that they asserted that they have no legal responsibility for what is put on their auction site. That is still the case.

Chairman SHAW. Well, maybe the Judiciary, Energy, and Commerce Committees should have a hearing on that. That is outside of our jurisdiction but I think it is something that really needs attention.

One last question and then we are going to have to go on. Where do they get all these numbers?

Mr. ROBINSON. Where do they get the Social Security numbers?

Chairman SHAW. Yes. I assume, Mr. Robinson, I assume from your testimony that you could obtain the Social Security number of anybody in this room that has one. And if that's the case, where did they get it?

Mr. ROBINSON. Most of the information that is provided by these sites is information not only from credit bureau headers but also from some publicly available documents, as well. What they do is there is a pool of information from these various sources and then they sell it to the public, anyone who would inquire for that information.

Chairman SHAW. But how can their information be so complete?

Mr. HUSE. All our lives we leave these markers as we negotiate loans, obtain loans, buy——

Chairman SHAW. Where is the clearinghouse for these markers? It seems like you have to go to so many sources in order to have a complete record that it would almost make it impractical to accumulate and put all this information into computers.

Mr. HUSE. The computers allow them to do it. Think of the credit applications you fill out for purchases of cars and so forth and homes. They are incredibly detailed. They give the story of your life and as this aggregates—a few years ago I had someone run my name in our office and the details were shocking. I mean they knew exactly in this database where I had lived throughout my life and who my neighbors were and what their income was. It is incredible. We have very little privacy left because of these databases. An amazing amount of information aggregates without our permission.

Chairman SHAW. Mr. Becerra has a follow-up.

Mr. BECERRA. Mr. Huse, we are not so much talking about the Social Security being misused. We are just talking about what you said before, a de facto national ID number that is being used, which happens to be the Social Security number.

Mr. HUSE. That is correct.

Mr. BECERRA. And what we are discussing here today under the rubric of the Social Security Administration's number is a national ID number and the fact that it is being abused and what happens when you have a universal system used to track your identity and information about you.

And if that is the case, this debate would take place whether or not we had a Social Security Administration and a Social Security number. It is the fact that that has become the de facto number that we are having this discussion but it would take place simply by the fact that we have now in a de facto world gone to the use of an identifier, a national identifier.

Mr. HUSE. Which is repugnant to most Americans.

Mr. BECERRA. Most people do not believe that or do not want to admit it but we have a national identifier.

Mr. HUSE. It has happened by accident and, to some extent, by intent but it has happened.

Mr. BECERRA. So, what we are discussing here is how we try to clean up the use of a national identifier?

Mr. HUSE. That is correct. And there are two approaches to this. The first is I think some of what we try to do or what you will try to do in your bill by allowing at least the number-holder to have some control over the migration of this information. I do not think that is unreasonable.

On the other hand, I think the Social Security Administration, because de facto, whether we like it or not, we control the issuance of these numbers. Although it was never intended to be a national identifier, we, and my office has recommended through its audit work that the Social Security number tighten up its process of enumerating people and they have made efforts to do that and those efforts continue, although more needs to be done.

I think the two pieces are about all we are really ever going to be able to do.

Mr. BECERRA. And how much of this that we are discussing today about the misuse of the number and the theft of identity has an impact on Social Security benefits themselves, what SSA is obligated to do? How much does this intrude on what you have to do in giving out benefits under Supplemental Security Income or Social Security retirement benefits? Are we into that area at all?

Mr. HUSE. Yes, we are. A lot of our fraud cases in Social Security are people who use bogus numbers or made up numbers or fake IDs. So there is a nexus there. It has a home with us at the OIG but also we have this unintended universal responsibility, too.

Mr. BECERRA. So one way or the other, whether this had become the national identifier or not, the Social Security Administration has to clean up the use of its own number for its own internal purposes because of the fraud committed within the Social Security Administration itself of people obtaining benefits fraudulently, et cetera.

Mr. HUSE. In our audit work—there are all kinds of issues here but in our audit work we have pointed out that Social Security's wage and earning information, which is critical to obtaining its benefits when those benefits come due, is flawed by the fact that it has a lot of this garbage number data in it. Our audit work has

proved that and for lots of reasons, the underground economy and so forth, that exists. But, I suggest that if we ever go to individual accounts we will really need to have a better handle on enumeration. The two are inextricably linked.

Mr. BECERRA. Thank you. Thank you, Mr. Chairman.

Chairman SHAW. I want to thank this panel. You have certainly given us a lot of things to think about. The world is far more dangerous out there than I think any of us have imagined and I appreciate very much your coming and giving us your time.

[Questions submitted from Chairman Shaw to the panel, and their responses follow:]

Social Security Administration
Office of the Inspector General
Baltimore, Maryland 21235
July 20, 2001

The Honorable E. Clay Shaw, Jr.
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives
Washington, DC 20215

1. In your testimony, you indicated the need for further legislation to prohibit the sale of Social Security number information, limit the use of Social Security numbers, provide sanctions for violations, criminalize the sale and purchase of the Social Security number and expand the Civil Monetary Penalty authority under the Social Security Act to include misuse of the Social Security number. Do you believe the bipartisan legislation recently introduced by certain Members of this subcommittee, H.R. 2036, adequately addressed your concerns? Is there anything else you believe should be included?

H.R. 2036 goes a long way toward what I described in my testimony as "putting the SSN back in its box." Given my position as Inspector General of the Social Security Administration, my perspective on this issue is a conservative one. My mission is to protect the integrity of the SSN, so I naturally favor more legislation, tighter restrictions, and more limited uses. For example, the use of the SSN as an identification number by private institutions such as hospitals and colleges creates a risk that those numbers will be misappropriated and misused. The investigation I cited in my testimony involving the sale of SSNs through an Internet auction site resulted from the theft of names and numbers from a private college. While H.R. 2036 would provide a means of punishing the online vendor of these numbers, it would not address the compilation, use, and storage of this information by the college. Similar uses of the SSN abound, and while I am certainly aware that competing interests must be weighed in the preparation of legislation, my mission is such that I will always favor a more restrictive approach to SSN use. That said, I am very happy to see the restrictions that H.R. 2036 does provide. The limitations it imposes are long overdue and will provide my office and others in law enforcement with significant tools in combating SSN misuse and identity theft.

2. You mentioned in your testimony that you are currently involved with another Federal agency in an investigation involving an Internet auction site. You also stated that the sale of the Social Security numbers over the Internet should be made illegal. Do the provisions in H.R. 2036 adequately address this need in your view?

The gentlemen who attempted to sell hundreds of names and SSNs over the Internet did so without significant fear of criminal prosecution. H.R. 2036 provides the criminal, civil, and administrative sanctions we so badly need to deter people such as this, and to punish them when they remain undeterred.

3. You also indicated in your testimony that the sale of the Social Security number "through other means" should be outlawed. Could you elaborate as to what other means you are referring?

I was not referring to any other "means" in particular, but was merely seeking to avoid limiting my statement to Internet transactions. Not all theft of SSNs takes place in cyberspace. Legislation which prohibited only the sale of SSNs over the Internet would likely give rise to other "means" of making such transfers. For example, the sale of a CD-ROM containing thousands of names and SSNs and other per-

sonal information, if sold at a computer show or through an ad in a magazine, would not constitute an Internet transaction, but would be just as harmful.

4. You stated that the Federal government created the Social Security number and it is up to the Federal government to determine what are the appropriate and necessary uses of the Social Security number. How do you define appropriate and necessary uses?

As I stated above, my definition of "appropriate and necessary uses" would necessarily be skewed by my position as Inspector General of the Social Security Administration. For a Government official whose mission is to protect the integrity of the SSN to the greatest extent possible, the most logical answer for me to give would be that the only "appropriate and necessary" use would be for the administration of Social Security programs. Obviously, we are too far down the path to return to what was the SSN's original intended use. The income tax system relies on the SSN, as does the military, the bankruptcy courts, and other Federal benefit programs. Even these uses create risks and contribute to identity theft. Other Congressionally-mandated uses, particularly in the realm of financial transactions, are what swung the door wide and placed the SSN in the hands of the private sector. De facto uses ranging from use of the SSN for identification numbers in schools and hospitals to customer numbers or employee identification numbers in countless corporations across the company opened the door to misuse even wider. I could go on and on. Which of these uses is appropriate and necessary is not for me to determine, any more than it is the decision of the credit bureaus who so heavily rely on the free flow of SSN information, or the county governments that use the SSN for everything from land records to water bills. In my testimony, I suggest that the time has come to make these difficult determinations. All who are affected should have their say, but if I were to step outside of my role as Inspector General and propose a standard, it would be this: an appropriate and necessary use of the SSN is one which primarily benefits the holder of the SSN, not the entity seeking to obtain, use, or transfer it, and which prohibits any further use or transfer of the SSN without the holder's express consent.

5. From reading your's and others' testimony, it sounds like there are several powerful Federal agencies involved fighting identity theft. Is this too many or too few? How do they interact with the state and local agencies? Has that relationship helped to prevent crime or does it complicate enforcement?

I don't think that there are either too many or too few agencies involved. Each has its own area of expertise that is critical to the task. For example, the Federal Trade Commission's role is invaluable in that the FTC is in the business of imposing limitations on commerce and providing a remedy when those limitations are ignored. My office is intimately familiar with the issuance, use, and misuse of Social Security numbers in a wide variety of contexts, including identity theft. State and local agencies provide local knowledge and expertise, as well as much-needed resources and additional means of bringing violators to justice. To the extent that Identity Theft continues to grow, rather than being curtailed, I do not believe it is a problem with the agencies seeking to curtail it, or the relationships they enjoy. Rather, it is a matter of reducing the permissible uses of the SSN in the first instance, and then providing significant criminal, civil, and administrative sanctions for those who would exceed approved uses.

6. Preventing Social Security number identity theft in the Internet era is a monumental task. While the public has some appreciation of the problem, would you not agree that it is the lack of assistance and protection to bono fide victims that also erodes public confidence in their privacy?

Absolutely. The testimony of the two victims who appeared before the Subcommittee made that clear, as do the stories that we hear on a daily basis in the Office of the Inspector General.

7. You mentioned the number of potential allegations of Social Security number misuse violations as over 90,000 in 2000. With the Internet and other forms of telecommunications growing, can we realistically believe we can make a dent in identity fraud even with new laws on the books. Don't we also need better protection of the consumer after the crime is committed, allowing victims to clear their records and making business a partner in stopping further fraud and getting records cleared?

I believe that better laws can make a significant difference. As I state above, the two keys to reducing identity theft are restricting the uses of the SSN as much as is reasonably possible, and then providing criminal, civil, and administrative sanctions to punish those who ignore those restrictions and deter others from doing so. We cannot eliminate identity theft, but we can make a significant dent. However, I agree with your statement that victims must be given a way to emerge from the

identity theft nightmare and recover their good names, and this cannot be done without help from the private sector. The true impact of identity theft in the vast majority of cases is the devastation to an individual's credit history. The businesses which write and control that history, and who enjoy a privileged position with respect to the use of the SSN, must be willing participants in a system that will reduce the impact of identity theft on the victims, even as we in government work to reduce the number of victims.

Sincerely,

James G. Huse, Jr.
Inspector General of Social Security

New York City Police Department
New York, New York 10038

Reply to Congressional Subcommittee

1. We believe that the posting of Social Security numbers in "plain text" on the Internet is a potential danger to all of us. Criminals can use these search tools to find out other's personal information. The posting that was referred to in the testimony can best be explained via example. Detective Fabozzi received a call from a complainant who stated that her identity had been stolen and personal information was posted on the Internet at a virtual school. A virtual school is one that provides classes and training via the Internet. The woman who called our office felt confident that the point of compromise was the virtual classroom. The perpetrator used an address and other identifiers that were only associated with information she did input into the system to register for the class. Upon investigating the NYPD Computer Crimes found that the school posted the student's name, SS#, and credit card information in clear text on the school web page. We notified the school and explained the dangers of this type of posting and the school agreed to take down the web page posting this type of information. We believe that the searching for social security numbers should be limited to agencies that are searching for a "legitimate" purpose. The responsibility of deciding legitimacy is something left for elected officials. However, requests for credit information should be logged and notification should be made to the individual whose information was requested. By putting in these precautions, a victim of identity theft can see who is inquiring about their credit history and can quickly identify fraud. By logging these requests, it enables victims and law enforcement to identify a point of compromise. A point of compromise is a location that contains identifying information and the perpetrators use a vehicle to steal personal information. For example, a restaurant that has a corrupt employee that steals credit card information is considered a point of compromise; since the victim's credit card numbers stolen all came from that one restaurant. We have investigated many cases where the point of compromise is a gas station, doctor's office, banks and brokerage firms. The only way to limit these internal leaks is place passwords and logs on systems that contain such information and to conduct background checks on employees. In addition training corporations on the vulnerabilities of having this information readily available is a must.

2. We believe that steps should be taken to limit the printing of social security numbers on documents such as driver's licenses. In NYS, SS#'s are not used as an identifier for licenses. By limiting the display of SS#'s you are limiting an avenue for fraud. SS#'s should never be posted on checks. If a fraudster has a check, which includes a SS#, he will have account information victim's name and SS#. With that information an identity theft can occur.

3. When an identity theft victim comes to the NYPD for help, we give them the address, phone numbers of the three major credit bureaus. Additionally, we take a police report for criminal impersonation or grand larceny depending upon the circumstances and begin an investigation.

4. The credit bureaus control a vast amount of information on individuals and are the best agency suited to assist victims of identity theft. However, the credit bureaus must also be aware that people with credit problems may use the identity theft alibi to erase bad debt. Like all technology issues, it is a double sword.

5. According to the Federal Trade Commission and reports done by the Consumers Union and others, identity theft is the number one growing crime in America. Estimates have been made that in the US in 2000, there was estimated between 500,000 and 700,000 victims a year.

6. The problems associated with identity theft is the clearing up your good name. Victims can be denied credit such as a loan or have to pay higher interest rate since

their credit worthiness has been diminished. Other problems that we have seen is the looting of bank accounts by impersonating the victim with false identification. In 2000, Detective Fabozzi conducted a major investigation where individuals were stealing victim's identities and creating ficticious id cards and walked into local bank branches and withdrew money from the victim's accounts. The loss to over 200 victims was over 1 Million dollars. One perpetrator also was arrested using the victim's name and date of birth and was given an arrest number belonging to the victim of identity theft. Others learn of the identity theft when a car is bought, or leased and used in a crime or an accident report.

7. Social engineering is just a trick or deceit of obtaining information from someone that has information that the impersonator wants. For example, a pickpocket in NYC will obtain the drivers license number, dob and address of a victims and call a bank, impersonate a customer and obtain account information. Obviously this is a security breach and should not be done. However, untrained customer service representatives may give out this information.

8. The encryption and secure socket layer is a secure transmission of information. However, the data is stored and is available once it reaches its destination. The data warehouses that contain the information may be vulnerable to hackers. A buffer overflow attack is a common means to obtain privleges that enable a hacker to steal information. A victim of identity theft usually assumes that his identity was stolen over the internet, but a majority of our investigations show that the point of compromise is usually an insider at a corporation that has been paid off.

Sincerely,

Michael Fabozzi
Detective

[The attachment is being retained in Committee files.]

Chairman SHAW. The next panel we have is Charles Bacarisse, who is the Harris County District Clerk in Houston, Texas. Cory Kravit, a student at the University of Florida in Gainesville, Florida and, I might say, a former intern in my office that has a very interesting story to tell about how he put to use some of the information that he learned while serving here in my congressional office. Evan Hendricks, who is the Editor and Publisher of Privacy Times. Charles Dugan, who is a partner with Covington and Burling on behalf of Financial Services Coordinating Council. Mark Rotenberg, who is the Executive Director, Electronic Privacy Information Center. Ronald Plesser, who is a partner in Piper, Marbury, Rudnick and Wolfe on behalf of the Individual Reference Service Group (IRSG). And Paula LeRoy, who is President of the Pension Benefit Information Services, Tiburon, California. Edward Mierzwinski, who is the Consumer Program Director of the United States Public Interest Research Group.

This is a very large panel. We appreciate your presence here. We have each of your full statements. They will be made a part of the record and I would invite each of you to summarize as you might be comfortable.

Mr. Bacarisse, I am starting with you, sir.

STATEMENT OF CHARLES BACARISSE, DISTRICT CLERK, HARRIS COUNTY COURT, HOUSTON, TEXAS

Mr. BACARISSE. Thank you, Mr. Chairman. It is a pleasure to be before you and your Committee this afternoon.

As the district clerk, the clerk of the courts, for the third largest county in the United States, we hold approximately 6 million Social Security numbers in our, our case files. They are there because, due to State statute, we are required to collect that information on

divorce and family law cases primarily but also on some criminal cases, as well.

So you had asked a question earlier, where does this type of information reseller get this data? They get it, one source, from the courthouses all over the United States. We are in a sense an untapped mine resource for these information resellers. I get requests in our office practically on a monthly basis from some of these information resellers to package my data in a certain way and sell a copy to them on either computer tape. Some of the requests are to download it directly off the Internet to them.

We refuse those requests because they are too labor-intensive—that is our basis for refusing that request—and would require undue expense to local government to comply with that request. But that does not stop them or any other private citizen from walking into the courthouse door and requesting a copy of that final divorce decree or any other public document that is in our courthouse.

So I am sort of betwixt and between, if you will, in this very important issue. I am commanded by State law to acquire this information into our courthouse but then I am also commanded by State law to make this information publicly available. So clerks across the United States are in this same sort of position and it makes us quite uncomfortable, I might tell you.

Let me also just share another point with you, if I may, that I hope will resonate with the Committee as you consider your new legislation. We are generally local government. I speak here as a member of NACO, the National Association of Counties, and also as an elected official. I am sensitive to privacy and to the need to protect our customers' and our citizens' privacy. But there is also a huge cost that could be placed on local government to comply fully with some legislation that might be enacted or might be considered by the Congress.

Let me share with you some comments that my colleague, Mr. Michael Jeanes, who is the clerk of court in Maricopa County—that is Congressman Hayworth's home district—Michael sent some comments to me, as well, which I think are important to remember. He says, "We would only be able to protect the Social Security information contained within the existing court paper files by hiring a staff whose job would be to redact this information before allowing the public access to the file. In order to maintain our existing levels of public service we would require approximately 25 to 30 new staff and related clerk office accessories—space, equipment, and so forth—and the staff would be in place for the next 10 years. Salaries, benefits, space and equipment for at least 25 additional staffers for at least 10 years could run $1 million a year." My county is just a bit larger than Maricopa, but not much, and I would expect a similar financial impact.

To sum up, I would ask the Committee to consider carefully balancing the huge mandates that might be placed on local governments to comply with whatever the Congress believes needs to be done and I would hope that you would call on us and we would work closely with you and the Committee to construct legislation we can all live with and that could be enforced effectively at the local level. Thank you.

[The prepared statement of Mr. Bacarisse follows:]

Statement of Charles Bacarisse, District Clerk, Harris County Court, Houston, Texas

Mr. Chairman and distinguished members of the committee, I am honored you invited me to testify about such a huge issue as privacy. I know that many Americans expect the government to do something about it.

As the Clerk of Court for Harris County, Texas, I understand this issue. My office deals with emotionally charged data like conviction and divorce records, and we administer a child support registry, so I know how people value their privacy . . . and how some hide from their responsibilities.

I see two critical questions for your consideration at this hearing:

—By regulating the accumulation and use of Social Security Numbers, can something effective be done to enhance privacy and/or reduce identity theft?

—And, what are the costs—obvious and hidden—in trying to restrict the accumulation and use of Social Security Numbers?

I think the answer to the first question is, unfortunately, no. Regulating the accumulation and use of Social Security Numbers will not be effective. That horse left the barn, long ago. In fact, the government helped burn down the barn! Right now, the IRS requires employers and banks to collect the Social Security Numbers. In Texas' Family Code alone there are at least 11 statutes requiring the use of SSNs.

In the private sector, landlords, blood banks, doctors, hospitals, life insurance companies and others collect Social Security Numbers.

SSNs are so widely available that you can get 65 million of them for free on line. Try Ancestry.com and click on "Social Security Death Index." You can obtain the full name, Social Security Number and birthdate of a dead person—who won't complain about identity theft!

Information brokers have huge databases containing SSNs and other data. Suppose you banned all trafficking in Social Security Numbers. Would that deter identity thieves? Couldn't the databases operate offshore, like Internet gambling sites?

Tighter regulations on the use of Social Security Numbers will increase the burdens and costs on everyone while doing little or nothing to enhance anyone's privacy.

Every divorce case in my county eventually should contain the SSN of each party and any children—in more than one document! So does every order affecting a parent-child relationship, every wage withholding order and many other documents. That is a huge amount of numbers to safeguard.

We estimate the cost of redacting one document at $8.07, and last year more than 16,600 divorces were granted in Harris County. Each year we sell about 930,000 certified pages from family law cases. That's a lot of pages to check.

Michael Jeanes, the Clerk of Court for Maricopa County, AZ, the home of Congressman Hayworth, has calculated the cost another way. He asked me to pass along this comment:

"We would only be able to protect SSN information contained within existing court paper files by hiring a staff whose job would be to redact this information before allowing public access to the court file. In order to maintain our existing levels of public service, we would require approximately 25–30 new staff and related Clerk's Office accessories (space, equipment, etc.). This staff would be in place for at least the next 10 years."

Salary, benefits, space and equipment for at least 25 additional staffers for at least 10 years could run $1 million a year. My county is a bit bigger, and I expect the financial impact would be similar.

Although I don't favor of it, user fees perhaps could cover the huge cost of redaction, but who's going to make up for the child support that won't be collected? Social Security Numbers are used by the private sector collection services that succeed—where government has failed miserably—in locating dead-beat parents and collecting child support.

Look at government accountability. Open records and open courts greatly reduce the chances of corruption. How will the public and the press follow things if local governments redact vital SSNs?

Your advisory announcing this hearing says, "according to the (Social Security Administration), the SSN is the single-most widely used record identifier in the public and private sectors."

That genie is not going back in the bottle no matter how much the law threatens and burdens custodial parents, taxpayers, businesses and governments.

I want to leave the committee with this thought: As you begin writing legislation, remember that those of us in state and local government want to work collabo-

ratively and cooperatively with you to safeguard all our citizens' privacy. However, please bear in mind the fiscal and logistical costs involved in restricting the use of Social Security Numbers. Also, please keep in mind that whatever laws are passed must be effective and enforceable.

Thank you for inviting me.

Chairman SHAW. Thank you. Mr. Kravit?

STATEMENT OF CORY B. KRAVIT, CHAIRPERSON, STUDENT SENATE'S AD HOC COMMITTEE ON SOCIAL SECURITY PRIVACY, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA

Mr. KRAVIT. Good morning, Mr. Chairman and members of the Subcommittee. My name is Cory Kravit and I am currently a political science senior at the University of Florida. I am appearing before you today representing the University of Florida student body and specifically as the chairperson of the Student Senate's Ad Hoc Committee on Social Security Privacy. In addition, I have been appointed by the university provost to serve on the University of Florida Student ID Task Force.

I would like to thank you, Mr. Chairman, and the esteemed members of this Committee for conducting this hearing today on such a vitally important issue. As members of this Committee, you are intimately aware of how widespread the problem of identity theft through the misuse of individual Social Security numbers has become. The problems of identity theft are not only confined to the working members of our society. Identity theft has become an issue for the students of our nation's universities, as well.

Through the University of Florida Student Senate's Ad Hoc Committee on Social Security Privacy, we have worked very hard to protect the identities and privacy of the students of the University of Florida, as well as students enrolled at other universities throughout the State of Florida.

It has become painfully clear that due to the misuse of Social Security numbers, an increasingly large number of university students within the State of Florida and throughout this nation have had their identities stolen. In fact, in 1998 the local university police department arrested a desk clerk working for the Jennings Residence Hall located on the University of Florida campus after he stole the identities of 23 college students. The desk clerk was charged with mail theft and credit card fraud after illegally spending nearly $70,000 without the students' knowledge. According to the Gainesville Sun, Alachua County Sheriff's Detective Robert Gaff stated, "This kind of fraud happens all the time. It is just not always on this large scale."

In my testimony here today, I will endeavor to discuss the widespread use of Social Security numbers for identification purposes within the State University system and the State of Florida and more specifically at the University of Florida. In addition, it will be with a great sense of pride and accomplishment that I will provide the members of the Subcommittee with an update outlining our progress and efforts despite substantial economic and logistical barriers to change from a Social Security number-based identification

system to a system that provides all students, staff and faculty with a more secure level of privacy and security.

In 1966 Social Security numbers were first used at the University of Florida as a primary form of student identification. Over the last 35 years hundreds of thousands of students have been required to use their Social Security number for nearly everything on campus. In the 1970s, the Florida Board of Regents mandated that all public universities within the State of Florida use the student's Social Security number as their student ID number. It is hard to imagine, but as a result of this mandate there are quite probably millions of students and alumni within the State of Florida and elsewhere that currently have their Social Security numbers unsecured and waiting to become a tool of the unscrupulous identity theft practitioner.

It is the opinion of the University of Florida Ad Hoc Committee on Social Security Privacy that Social Security numbers should be used for only two purposes: financial aid application requirements and reports requested by States and Federal governmental agencies. Students at the University of Florida are required to provide their Social Security number for virtually everything ranging from registering for classes to ordering Little Caesar's pizza using one's student debit account.

For example, I have had to use my Social Security number to sign attendance sheets that are passed around the classroom, provide my Social Security number on exam grids and forms, purchase a parking decal to park on campus, qualify for student government elections and appointments, and one use that is most disturbing is that student Social Security numbers are routinely posted on grade sheets that are made public and become accessible via the Internet. The list goes on and on.

As a student preparing to enter my senior year I am currently in the process of applying to law schools and as part of this process my transcripts must be sent to the Law School Data Assembly Service who, by the way, require that my Social Security number be placed on every document sent to them.

Recently I took a summer class at Florida Atlantic University in my home town of Boca Raton. When paying for the transcripts to be sent back to the University of Florida the Florida Atlantic office staff specifically told me that I had to print my Social Security number on my check. Knowing what I do about identity theft, I cordially explained that I would prefer not to place my Social Security number on the check. I explained that a personal check with my account number and Social Security number printed on it was a con artist's dream and I would not allow myself to partake in such a risky practice. The university cashier grunted at me, rhetorically, I suppose, "Well, you do know this is your student ID number." She eventually accepted my check without my Social Security number printed on it. Hopefully, my transcripts will be sent without any flaws because I really do want to go to law school.

With everything that I have learned through my research into identity theft, I find that the scariest part of this equation is that students have become so accustomed to giving out their Social Security numbers, they instinctively offer it, even when it is not needed. Before I had had a chance to talk with the victims of identity

theft I used to print my Social Security number on virtually all my term papers, reports and exams. Students just do not realize how unique and vulnerable their Social Security number is. I work part-time for the long distance telephone service on the University of Florida campus. My job brings me into contact with fellow students who come to pay their telephone bills. Not a day goes by that at least one student needs me to look up their account information and they ask me if I need their Social Security number. Of course, I explain to them the potential for disaster but unfortunately, many cannot understand the magnitude or the problem or perhaps they just do not care.

So you may ask, who has access to our Social Security numbers? The answer is alarming. Pretty much anybody who requests them. Just last week a friend of mine phoned me infuriated that his girlfriend's professor printed her entire class's full nine-digit Social Security number on the class's Internet website. This act, although done with no malice or ill intent, could possibly lead to identity theft of every student in that class. I am so highly concerned with this issue that I have printed a copy of the class website for the members of the Subcommittee to review. Yes, it is just that easy.

Con artists rarely need to put forth much effort. When you think about it, the Social Security number of each and every student is freely available to numerous individuals within the university. This list includes professors, teaching assistants, dormitory desk clerks, resident assistants, registrar staff, library staff, Little Caesar's Pizza employees, book store employees, mail carriers, and the general student body.

The bottom line is that students in this country are at an increased risk for identity theft due to the often unrestricted and free use of their Social Security numbers within our country's university system. The average student might not realize that he or she were a victim of identity theft because many students do not have credit cards and have never applied for a loan and have not checked their credit histories. Students could graduate and leave for their new jobs, only then realizing that their credit has been destroyed.

I have worked hard this past school year to recommend that the University of Florida administration abandon their current practice of using individual Social Security numbers as student identifiers. The university administration, despite the obvious economic and logistical barriers to such a change, has responded in a remarkable fashion. In January the university provost appointed representatives from all the major departments to the Student ID Task Force. I am currently a member of this task force and we are working to develop a state-of-the-art directory system that would only give those who absolutely need a student's Social Security number access to it. A random public ID number will be used for all other university transactions.

Although it may seem like a simple project, it is not. To revamp the database, at the University of Florida alone it has been compared to the Y2K project squared. New computer programs must be written, new forms will need to be printed and over 50,000 students, faculty and staff need to be advised of the new system once it is put in place.

Mr. Chairman and the esteemed members of the Committee, there are many schools and universities across the United States that are just like the universities within the Florida State University system. These schools continue to use their students' Social Security numbers as their primary student ID numbers. Unfortunately, Representative Doggett is not present here today. However, the University of Texas in his district happens to be one of these schools. A student reporter from the University of Texas recently wrote a week-long special report on identity theft and how students are severely affected. It is currently perfectly legal for universities in this nation to continue the practice of using a student's Social Security number as his or her student ID number. Many schools cannot afford to change their database systems even if they wanted to. I believe that the proactive efforts of your Subcommittee will have a great effect at exponentially reducing the risk of identity theft that is now associated with students attending the colleges and universities of this nation.

With my most sincere admiration and respect, thank you very much for your time.

[The prepared statement of Mr. Kravit follows:]

Statement of Cory B. Kravit, Chairperson, Student Senate's Ad Hoc Committee on Social Security Privacy, University of Florida, Gainesville, Florida

Good morning Mr. Chairman, and the members of the Subcommittee. My name is Cory B. Kravit and I am currently a Political Science senior at the University of Florida. I am appearing before you today representing the University of Florida student body and specifically as the Chairperson of the Student Senate's Ad Hoc Committee on Social Security Privacy. In addition, I have been appointed by the University Provost to serve on the University of Florida's Student ID Task Force.

I would like to thank you Mr. Chairman, and the esteemed members of this committee for conducting this hearing today, on such a vitally important issue. As members of this committee, you are intimately aware of how widespread the problem of identity theft through the misuse of individual Social Security numbers has become. The problems of identity theft are not only confined to the working members of our society, identity theft has become an issue for the students of our nation's universities as well. Through the University of Florida Student Senate's Ad Hoc Committee on Social Security Privacy, we have worked very hard to protect the identities and privacy of the Students at the University of Florida, as well as students enrolled at the other universities throughout the State of Florida.

It has become painfully clear that due to the misuse of Social Security numbers an increasingly large number of University students within the State of Florida and throughout this nation have had their identities stolen. In fact, in 1998 the local university police department arrested a desk clerk working at the Jennings Residence Hall located on the University of Florida campus after he stole the identities of 23 college students. The desk clerk was charged with mail theft and credit card fraud after illegally spending nearly $70,000 without the students' knowledge. According to the Gainesville Sun, Alachua County Sheriff's Detective Robert Gaff stated, "This (kind of fraud) happens all the time, it's just not always on this large scale."

In my testimony here today, I will endeavor to discuss the widespread use of Social Security numbers for identification purposes within the State University System of the State of Florida, and more specifically at the University of Florida. In addition, it will be with a great sense of pride and accomplishment that I will provide the members of this subcommittee with an update outlining our progress and efforts despite substantial economic and logistical barriers to change from a "Social Security Number" based identification system, to a system that provides all students, staff and, faculty with a more secure level of privacy and security.

In 1966, Social Security numbers were first used at the University of Florida as the primary form of student identification. Over the last thirty-five years, hundreds of thousands of students have been required to use their Social Security number for nearly everything on campus. In the 1970's the Florida Board of Regents mandated

that all public universities within the State of Florida use a student's Social Security number as their student ID number. It is hard to imagine, but as a result of this mandate, there are quite probably millions of students and alumni within the State of Florida and elsewhere that currently have their Social Security Numbers unsecured and waiting to become a tool of the unscrupulous identity theft practitioner.

It is the opinion of the University of Florida Ad Hoc Committee on Social Security Privacy, that Social Security numbers be used for only two purposes: financial aid application requirements and reports requested by State and Federal governmental agencies. Students at the University of Florida are required to provide their Social Security numbers for virtually everything ranging from registering for classes to ordering a Little Caesar's pizza using one's student debit account.

For example I have had to use my Social Security number to:

- Sign attendance sheets that are passed around the classroom.
- Provide my Social Security number on exam grids/forms.
- Purchase a parking decal to park on campus.
- Qualify for Student Government elections and appointments
- And one use that is most disturbing is that student Social Security numbers are routinely posted on grade sheets that are made public and become accessible to the world via the internet

The list goes on and on.

As a student preparing to enter my senior year, I am currently in the process of applying to law schools. As part of the process, my transcripts must be sent to the Law School Data Assembly Service, who by the way require that my Social Security number be placed on every document sent to them.

Recently, I took a summer class at Florida Atlantic University in my hometown of Boca Raton. When paying for the transcripts to be sent back to the University of Florida, the Florida Atlantic University office staff specifically told me that I HAD to print my Social Security number on the check. Knowing what I do about identity theft, I cordially explained that I would prefer not to place my Social Security number on the check. I explained that a personal check with my account number and Social Security number printed on it was a con artist's dream and I would not allow myself to partake in such a risky practice. The University cashier grunted at me (rhetorically I suppose) "Well you do know it is your student ID number." She eventually accepted my check without my Social Security number printed on it. Hopefully my transcripts will be sent without any flaws, I really do want to go to law school.

With everything that I have learned through my research into identity theft, I find that the scariest part of this equation is that students have become so accustomed to giving out their Social Security numbers, they just instinctively offer it even when it is not needed. Before I had a chance to talk with victims of identity theft, I used to print my Social Security number on virtually all my term papers, reports and exams. Students just don't realize how unique and vulnerable their Social Security number is. I work part time for the long distance telephone service on the University of Florida Campus. My job brings me into contact with fellow students who come to pay their telephone bills. Not a day goes by that at least one student needs me to look up their account information and they ask me if I need their Social Security number. Of course I explain to them the potential for disaster but unfortunately, many cannot understand the magnitude or the problem or perhaps they just do not care.

So you may ask, who has access to student Social Security Numbers? The answer is alarming . . . pretty much anybody who requests them. Just last week a friend of mine phoned me infuriated that his girlfriend's professor printed her entire classes full nine digit Social Security number on the classes Internet website. This act, although done with no malice or ill intent could possibly lead to the identity theft of every student in that class. I am so highly concerned with this event, that I have printed a copy of the class website for the members of this Subcommittee to review. Yes, it is just that easy. Con artists rarely need to put forth much effort. When you think about it, the Social Security number of each and every student is freely available to numerous individuals within the university. This list includes professors, teaching assistants, dormitory desk clerks, Residence Assistants (RA's), registrar staff, library staff, Little Caesar's Pizza employees, bookstore employees, mail carriers, and the general student body.

The bottom line is that students in this country are at an increased risk for identity theft due to the often unrestricted and free use of their Social Security numbers within our country's University system. The average student might not even realize that he or she were a victim of identity theft because many students do not have credit cards, have never applied for a loan, and have not checked their credit his-

tories. Students could graduate and leave for their new jobs, only then realizing that their credit has been destroyed.

I have worked hard this past school year to recommend that the University of Florida administration abandon their current practice of using individual Social Security numbers as student identifiers. The University administration, despite the obvious economic and logistical barriers to such a change has responded in a remarkable fashion. In January, the university provost appointed representatives from all the major departments to the Student ID Task Force. I am currently a member of this task force and we are working to develop a state of the art directory system that will only give those who absolutely need a student's Social Security number access to it. A random public ID number will be used for all other university transactions. Although it may seem like a simple project, it is not. To revamp the database at the University of Florida alone has been compared to the Y2K project squared. New computer programs must be written, new forms will need to be printed, and over 50,000 students, faculty, and staff need to be advised of the new system one it is put in place.

Mr. Chairman and esteemed committee members, there are many schools and universities across the United States that are just like the universities within the Florida State University System. These schools continue to use their students Social Security numbers as their primary student ID numbers. Representative Doggett, I believe that the University of Texas in your district happens to be one of these schools. A student reporter from the University of Texas recently wrote a weeklong special report on identity theft and how students are severely affected. It is currently perfectly legal for the Universities in this nation to continue the practice of using a student's Social Security number as his or her student ID number. Many schools cannot afford to change their database systems even if they wanted too. I believe that the proactive efforts of your Subcommittee will have a great affect at exponentially reducing the risk of identity theft that is now associated with student's attending the colleges and universities of this nation.

With my most sincere admiration and respect, thank you very much for your time.

[The attachments are being retained in the Committee files.]

Chairman SHAW. Thank you. Mr. Hendricks?

STATEMENT OF EVAN HENDRICKS, EDITOR/PUBLISHER, *PRIVACY TIMES*

Mr. HENDRICKS. Thank you, Mr. Chairman and members of the Committee. Like most personal data, the Social Security numbers are not adequately protected by law and in order for the American people to have the legal protection they deserve there must be political leadership on the issue. Mr. Chairman, your continuous efforts to pass an SSN privacy bill are an example of the kind of leadership that will be necessary if Americans' right to privacy is to be effectively protected.

I am on the Social Security Administration's privacy advisory panel. I have also been qualified by the courts as an expert on identity theft. One thing we have seen in several cases is that the use of the Social Security number actually helps facilitate fraud because if the real person, the victim has the name of Myra Coleman and the imposter's name is Maria Gayton and she uses the same Social Security number, the algorithm actually allow the data to match and for the credit reports to be disclosed because there is enough similarities between Myra and Maria and Coleman and Gayton.

So, the Social Security number in some of these cases actually facilitates fraud, which is why I am here to urge you to enact a very strong bill with limited exceptions. There will be a concerted lobbying effort for exceptions to this bill; that can always be ex-

pected. But, if there are to be exceptions they should be narrowly drawn and if there is rulemaking, the bill should clearly state what the standards are to remove ambiguity for the agency rule-makers.

Furthermore, I think the Subcommittee needs to proceed with the explicit recognition that in general, Americans' privacy is not adequately protected in law or in organizational practice and that more comprehensive legislative and organizational solutions are needed. The Subcommittee therefore should declare its SSN bill as a vital piece of a larger privacy policy that Congress and the president owe to the American people.

There is a myriad of reasons why this is a great place to start. One of the reasons is the Social Security number is an example of what went wrong with privacy. Slowly but surely the number was used for purposes other than what it was originally intended for. The promise that the Social Security card would not be used for identification turned out to be a lie to the American people. So this is an exercise in restoring trust and rebuilding trust with the American people, and should be part of a larger effort that needs to be made with the use of personal information and with privacy.

The problems with the Social Security number were recognized back in 1976 by a presidential study commission called the Privacy Protection Study Commission. My fellow panel member, Ron Plesser, was the general counsel of that commission. They did some excellent work. Though they did not at that time recommend restrictions on the SSN in the private sector, mainly because it was not being used that widely in the private sector, they saw a clear danger that a government record system such as that used by the SSA or the IRS could become a de facto central population register unless prevented by conscious policy decisions.

Unfortunately, there were not conscious policy decisions and what they feared is what has happened. They made several recommendations, including the establishment of a permanent privacy commissioner to monitor the issue. But, their recommendations probably seemed somewhat esoteric at the time when they talked about fears about privacy. Now we see that the fears are not esoteric because the failure to protect privacy is directly tied to the facilitation of fraud and identity theft is the fastest growing crime in the information age. This makes sense. As the detective said, it is a low risk, high pay-off crime.

Legislation is urgently needed to address this issue. We should ban the sale of Social Security numbers in the private sector to stop what we saw this morning. We should prohibit the sale and display of SSNs by Federal, State and local government agencies, the Department of Motor Vehicles (DMVs).

Another thing, we should take from the Privacy Act and place a duty on organizations. If they are going to collect Social Security numbers, particularly like life insurers and health insurers, then they have to take reasonable or appropriate steps to protect the security and privacy of that data. They cannot enjoy what they think are the benefits of collecting the SSN without assuming the responsibility for protecting it, and that standard could be lifted directly out of the Privacy Act.

Basically, in terms of solutions it is going to come down to purpose tests. Good purposes should be allowed; bad purposes should

be prohibited. But the current situation where any purpose goes is clearly unacceptable, both for privacy and for fighting fraud.

The FTC's agreement with the Individual Reference Service Group (IRSG) companies in my view has turned out to be totally ineffective. I could answer more questions about that in the question period.

The other thing, and it is not in my prepared statement but I just found this out last night, that industry is already preparing for life after any law that would restrict the sale of credit headers by simply working harder to collect the information from the public records, making separate databases there. And so if you only prohibit credit header data they will create a new silo, housing the information from public records.

There are some important lessons from the last Congress. One is that there will be a concerted lobbying effort looking for exceptions. This is all the more important because we have had three excellent court decisions, one by the Federal appeals court here, one by the Federal district court and one by the State court in Washington State, saying that the Social Security number deserves protection and there is no First Amendment right to traffic in Social Security numbers without people's consent.

At the beginning of the statement I spoke of the importance of political leadership. Unfortunately, a second lesson from last Congress is that the House Republican leadership has emerged as one of the main obstacles to privacy legislation. Last year sources told me the leadership was unwilling to allow privacy bills such as the chairman's to advance to the House floor. The speaker, J. Dennis Hastert, has denied Americans need for stronger protections. They say we should not legislate new laws for the private sector until the Federal Government cleans up its own systems to safeguard our citizens' personal information.

Well, of course we should clean up the Federal Government but Americans want their privacy protected and they are not going to feel any better if it is being invaded by a private sector organization. Opinion poll after opinion poll show they want stronger protections. I can provide further information for the record.

President Bush has made some very positive comments about the need to protect privacy and in his only action he has allowed the medical privacy rules to go forward, giving them a green light. But what is really needed is for the president to walk the walk now and come forward with a comprehensive legislative proposal for a national privacy policy. The American people want this and they are expecting it.

The final comment I would like to say is that though you will hear loudly from the businesses that say privacy will negatively impact, there are a lot of forward-looking businesses that see privacy as integral to their business models. This includes the wireless communications industry and Microsoft's Hailstorm because they know that their business model depends on having consumer trust and being able to leverage personal information and using technology so it can serve individuals. So, privacy is actually a very pro-business issue now and increasingly recognized as one.

And the final point I would like to make is as high-level policymakers, members of Congress, should understand that there are

tremendous savings from moving into the electronic realm. Paper is slow and expensive and it is driving up costs for our Federal agencies, for large businesses and for banks. And so by moving into the electronic realm we can have tremendous savings on the bottom line for our largest organizations. That simply will not happen unless we have privacy trust and that will require a privacy-first policy. Thank you very much.

[The prepared statement of Mr. Hendricks follows:]

Statement of Evan Hendricks, Editor/Publisher, *Privacy Times*

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify on the important issue of protecting the privacy and preventing the misuse of Social Security numbers (SSNs).

Like most of other personal data, the privacy of Americans' SSNs is not adequately protected by law. In order for the American people to have the legal protection they deserve, there must be political leadership on the issue. Mr. Chairman, your continuous efforts to pass an SSN-privacy bill are an example of the kind of leadership that will be necessary if Americans' right to privacy is to be effectively protected.

By way of introduction, I am Evan Hendricks, Editor/Publisher of Privacy Times, a Washington newsletter that I founded 21 years ago. I have been qualified by federal courts as an expert on identity theft in Fair Credit Reporting Act cases. I currently serve on the Social Security Administration's expert panel on privacy, assisting the SSA formulate and apply Privacy Impact Analyses to existing and contemplated electronic services.

I am here to urge the Subcommittee to enact a bill that bans the sale of SSNs, particularly in "credit headers," and prohibits organizations from coercing individuals from divulging their SSNs as a condition of service. Most importantly, there should be few, if any, exceptions. I expect that what will follow this hearing is a concerted lobbying effort by organizations to be exempted from the bill's restrictions. If there are to be exceptions, they must be narrowly tailored. If the bill mandates agency rulemaking, the bill's standards should be clearly stated so as to remove ambiguity for agency rulemakers.

Moreover, I urge the Subcommittee to proceed with an explicit recognition that, in general, Americans' privacy is not adequately protected in law or in organizational practice, and that more comprehensive legislative and organizational solutions are needed. The Subcommittee therefore should declare its SSN bill as a vital piece of a larger privacy policy that Congress and the President owe to the American people.

There are a myriad of reasons why Congress should move aggressively and comprehensively to protect privacy. A main philosophical reason is to restore and build trust between citizens and the institutions with which they must deal in the course of daily life. For a major aspect of trust in the information age is assuring citizens that their personal data will only be used in a fair manner, based upon their informed consent and that is consistent with their expectations.

There are several reasons why the SSN is a logical starting point for creation of a more comprehensive national privacy policy.

Background

The Social Security Card used to state: "This card is not to be used for identification." The promises in the early days that the SSN would not become an identification number has turned out to be one of the great lies to the American people.

Clearly, the history of the SSN is a classic case study in the erosion of privacy. The SSN has proved to be the valuable key element that allows computer to talk to each other, to search through each other's data files and to draw out individual profiles on people. Accordingly, the 1960s-era worry of one, centralized computer system on all Americans is no longer the only concern. Now the interconnection of small and large computer networks, made easier by widespread use of the SSN, coupled with the advent of the Internet, has created 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 agen-

cy 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. By 1990, about three dozen States used the SSN as a driver identification number. This meant that the number often was recorded on checks as an ID number when consumers made purchases. The1976 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 their SSNs to financial institutions so IRS computers could match the amount of interest reported back to 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 required parents to show SSNs for children over the age of five who are claimed as dependents.

By 1990, it became common for a wide array of private sector organizations to rely on the SSN as a customer identifier even though it was not required. These included utilities, insurance companies, health care providers, video rental outlets and universities.

The expanding use of the SSN was contrary to the goals of the Privacy Act of 1974. Section 7 of the Act ostensibly prohibits Federal, State or local agencies from requiring the SSN as a condition of a governmental service or benefit. But as we have seen, that prohibition, to some extent, has been trumped by subsequent actions. (Marc Rotenberg, of the Electronic Privacy Information Center, will address the Privacy Act more fully in his testimony.)

Moreover, the U.S. Privacy Protection Study Commission (PPSC) in its 1976 report to Congress warned that the SSN could, if unchecked, become a convenient tool for invading privacy. The SSN's use was not as widespread in the private sector in 1976. For instance, TRW, the major credit bureau, did not use it as its main identifier then for credit reports. Although the PPSC did not call for restrictions on private sector use of the SSN, it saw 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 unless prevented by conscious policy decisions."

The PPSC made four recommendations concerning the SSN:

(1) Keep the Privacy Act's Section 7 restrictions;

(2) The President issue a new Executive Order rescinding President Roosevelt's E.O. authorizing agencies to rely on the SSN as an individual identifier—in essence, a moratorium on new uses by federal agencies;

(3) That Congress create an independent entity, a permanent Privacy Commissioner, which would have many duties, including monitoring SSN developments and recommending new restrictions.

(4) "That the Federal government not consider taking any action that would foster the development of a standard, universal label for individuals, or a central population register. . . .

Events of the past two decades have validated the PPSC's concerns and recommendations. Yet at the time, the fear that people's data theoretically could be merged and used in ways that would threaten privacy was a bit too esoteric to have much impact.

The New Paradigm: Identity Theft

What virtually nobody realized was that the failure to protect the privacy of personal data and the SSN would make possible what soon became the fastest growing crime of the information age: Identity Theft. The first piece of data an identity thief wants is the SSN. Identity theft occurs when an imposter steals a consumer's identity, usually a Social Security number and sometimes a name and address, for the purpose of exploiting the credit-worthiness of an innocent consumer, obtains credit in the name of the innocent consumer, and absconds with goods. This activity leaves the innocent consumer with the debris of a polluted credit history.

Identity theft was becoming an epidemic before the Internet became popular. The steady rise in the number of identity theft cases has been well documented. In May 1998, the General Accounting Office, relying on figures provided by the Trans Union

Corp., reported that the number of consumer inquiries to Trans Union's fraud desk grew from 35,235 in 1992, to 80,013 in 1993; to 154,365 in 1994; 265,898 in 1995, 371,220 in 1996 and 522,922 in 1997. Trans Union estimates that about two-thirds of these inquiries relate to identity fraud. Two more recent sources of statistics—the Federal Trade Commission and California police agencies—indicate the epidemic is worsening. The problem promises to worsen because there are indications that organized crime gangs are gravitating towards identity theft as a "low-risk, high payoff crime."

What we are waiting to see is confirmation that identity thieves are regularly buying SSNs and other personal data from information brokers.

Legislation Urgently Needed

While comprehensive legislation is needed to protect privacy across many sectors, the ultra-sensitive SSN warrants specific action now. An SSN-centric bill should be seen as the leading piece of a larger legislative effort.

Here are some goals that SSN-privacy legislation should achieve:

- Ban the sale of SSNs by the private sector, particularly as part of credit headers.
- Prohibit the sale and display of SSNs by Federal, State and local governments.
- If not an outright ban on the use of SSNs as a driver's license number, then mandate that DMVs can only use the SSN if the driver opts in, as is currently practiced in the District of Columbia.
- Place a duty on all organizations that collect and maintain SSNs to establish appropriate administration, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(This standard is from the U.S. Privacy Act of 1974).

I also agree with the more detailed comments on the bill that will be made by Ed Mierzwinski, of the U.S. Public Interest Research Group, in the next panel.

Lessons From Last Congress

There were two central lessons from efforts in the last Congress to pass legislation to restrict uses of SSNs. The first is that a relatively small circle of companies, generally known as the IRSG Group, which hopes to continue trafficking in SSNs and personal data without the individual's consent, will lobby ferociously to preserve their free ride. Since it is not practical to oppose the bill outright, their strategy is to win enough exceptions so that the exceptions can swallow the statute. Indeed, last year, the Senate bill ultimately was riddled with so many loopholes that Amy Boyer's parents asked that their daughter's name not be associated with it.

Last year made it clear that a bill containing anti-privacy exceptions and loopholes will not pass.

It is particularly important to resist loopholes in light of two recent court rulings that have strengthened the consensus that personal data, credit headers and SSNs are protected federal privacy laws. The first ruling was by the U.S. Court of Appeals for the District of Columbia, and related to Trans Union's unsuccessful bid to continue selling credit header to marketers, even though it is prohibited by the Fair Credit Reporting Act and opposed by the FTC. The second ruling concerned Judge Ellen Segal Huvelle's rejection of the IRSG companies' challenge to the FTC privacy rule on credit headers. In both cases, the courts said the two laws reasonably furthered a substantial governmental interest in protecting privacy, and that the laws did not impinge on the companies' First Amendment right to commercial speech.

A Washington State judge ruled in May that a Web site did not have a First Amendment right to post the SSNs of law enforcement officers because SSNs lack a "substantive communicative purpose" and, therefore, lack Constitutional protection.

Mr. Chairman, at the beginning of my statement, I spoke of the importance of political leadership to Americans gaining the privacy rights they deserve. Unfortunately, a second lesson from last Congress is that the House Republican Leadership has emerged as one of the main obstacles to privacy legislation. Last year, sources told me that the Leadership was unwilling to allow privacy bills such as yours to advance to the House Floor.

This year, Speaker J. Dennis Hastert incredibly denied that Americans need stronger privacy protection, stating, "We should not legislate new laws for the pri-

vate sector until the Federal government cleans up its own systems and safeguards our citizens' personal information."

It's difficult to see the logic in this. Sometimes Big Government invades our privacy; sometimes it's the private sector. Americans want their privacy protected—period. It's of little comfort to them if the mega-institution improperly using their data is a private business, and not the government. And besides, even those who say they only care about governmental invasion of privacy need to be concerned about data collection by the private sector, because government agencies have shown time and again that they are perfectly happy to "piggyback" off of data collected by businesses. Moreover, privately held data are usually only a subpoena away from being discovered by a civil or governmental attorney.

The Leadership's position against privacy is a classic example of those, who by virtue of climbing the power ladder in Washington, seem to lose touch with the American people. In opinion poll after opinion poll, study after study, the American people have made it clear that: (1) they feel they are losing control over their personal information; (2) they don't feel current law or practice adequately protects their privacy and (3) they want more and stronger legal safeguards for their personal data.

At best, it's a mystery as to how the Leadership can continue to ignore the overwhelming evidence that Americans want their privacy protected, and that adequate law is necessary. At worst, it's a case of narrow special interests and their lobbyists controlling Washington against the wishes of the American people.

President Bush

In contrast to the House Leadership, President Bush has made strong pro-privacy statements, particularly about the need to protect medical and financial records—and yes, Social Security numbers. According to the Wall Street Journal, the President said he's "a privacy kind of guy." White House spokesman Ari Fleisher said the President will "tend to side with the privacy point of view" over business, and that, "It's good for business to honor people's privacy."

These statements came out in April when the President decided to approve final adoption of the medical privacy rules—his first and only action to date on privacy. This is a good first step. But now the President should be ready to "walk the walk," and prepare a comprehensive legislative package for a national privacy policy. As I said before, Mr. Chairman, your SSN bill is a good starting point for the larger effort.

Privacy Integral To Future Business Success

The irony is that there is a growing realization among forward-looking corporations that privacy is integral to future business success. This is because many corporations are developing technology, products and services that will bring new conveniences to consumers. But for these products to work, consumers must be willing to trust their personal data and profiles to a company's electronic information system. These corporations understand there must be credible and enforceable privacy protections in place if consumers are to provide personal data on which the business model rests. Examples include the Wireless communications industry and their plans for "3G" and location-based services, and Microsoft's Hailstorm.

In addition, a review of the Internet's recent boom-to-bust cycle make clear that e-tailers did not make their numbers, in part because consumer concerns about 1) credit card security and 2) personal data privacy, made them reluctant to purchase online. I am convinced that to the extent we put in place a strong privacy regime is the extent to which we will accelerate e-commerce.

Privacy Will Prevail Because We Can't Afford Otherwise

Shuffling paper is expensive and slow. Collecting and storing data and transacting electronically is much more cost effective, more convenient and faster. It probably costs the Social Security Administration a few dollars a piece to mail out checks or earnings statements, or process benefits claims—on paper. To do these same tasks electronically costs pennies apiece.

Similarly, the Internal Revenue Service could reduce its costs by hundreds of millions—if not billions—if it could convince higher percentages of taxpayers to file electronically. The same could be said for virtually any government benefits program.

Many corporations also could significantly reduce their bottom line costs if they could switch customers from a primarily paper environment to a primarily electronic environment. A recent survey by the TowerGroup found that 92 percent of the 3,033 households had used bank branches for transactions in the previous month. Only 18 percent of the households whose primary banks offered online services had actu-

ally used them, and even 85 percent of those said they also had visited a bank branch in the previous month.

As was with e-commerce generally, privacy concerns pose a major barrier to Americans utilizing electronic services of government agencies or businesses. These concerns are not irrational. People saw that their privacy was not adequately protected in the pre-Internet age. The government essentially lied about the SSN only being for Social Security and wage reporting. People see their own names arrive in the form of junk mail from organizations they never heard of and then are unable to find out where these organizations got their names. People are assaulted at the dinner hour with annoying junk phone calls. Their credit reports are often plagued by inaccuracies. Identity theft has become an epidemic. And recently, there have been regular reports of specialized hackers, known as "Carders," hacking into databases to steal thousands of credit card numbers at a time.

It is high time that we realize that the majority of Americans are not going to opt for electronic services until they are convinced that the privacy and security of their personal data will be protected by law and by organizational practice. This means that government agencies and corporations will continue to incur the higher costs of paper-based processing. It also means that many consumers will be deterred from the speed and convenience of electronic services.

I believe it is in our national interest to create an environment where organizations and individuals can enjoy the benefits of conducting business electronically. But in order to create that environment, we must show Americans that we are making a break with the past: namely, the United States is leaving behind its national policy of "Privacy-Neglect," and adopting a national policy of "Privacy-First."

In trying to hold off privacy legislation, certain industries are producing "Cost studies" in an effort to show that complying with privacy law is too expensive. Two of the more shameless examples were the "study" produced by Ernst & Young for the Financial Services Roundtable, and the one conducted by Robert Hahn, paid for by the Association for Competitive Technology. Neither one of these studies will stand up to independent scrutiny. For example, neither of the studies acknowledged there was any benefit to privacy protection.

What we need is independent, authoritative research that can evaluate the benefits and savings of a "Privacy-First" national policy that will create an environment of trust for electronic services.

Mr. Chairman, again, thank you for this opportunity to appear before the Subcommittee.

I'd be happy to answer any questions.

[The attachment is being retained in the Committee Files.]

Mr. COLLINS. [Presiding.] Thank you, Mr. Hendricks. I hated to use the gavel but I thought you might have a third final. Mr. Dugan?

STATEMENT OF JOHN C. DUGAN, PARTNER, COVINGTON & BURLING, ON BEHALF OF FINANCIAL SERVICES COORDINATING COUNCIL

Mr. DUGAN. Thank you, Mr. Chairman and members of the Subcommittee. My name is John Dugan. I am a partner with the law firm of Covington & Burling, and I am testifying today on behalf of the Financial Services Coordinating Council, or FSCC, whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, Investment Company Institute and the Securities Industry Association.

The FSCC represents the largest and most diverse group of financial institutions in the country, consisting of thousands of large and small banks, insurance companies, investment companies and securities firms. Together, these financial institutions provide financial services to virtually every household in the United States.

The FSCC very much appreciates the opportunity to testify today. While we recognize that there have been misuses of Social

Security numbers, we strongly urge that any legislation intended to address this problem be carefully targeted to specifically identify abuses, such as measures to stop identity theft. We believe it is imperative to avoid restrictions on legitimate and beneficial uses of Social Security numbers.

Let me summarize our written testimony by making three fundamental points. First, businesses' legitimate use of Social Security numbers as unique identifiers of individuals is now woven into the very fabric of commercial transactions throughout the country. Realizing the enormous value of a common, unique identifier, the Federal Government began the use of Social Security numbers for unrelated identification purposes nearly 60 years ago. It soon required businesses to do the same thing under certain Federal laws.

Businesses, including financial institutions, have followed the government's example and have used Social Security numbers as common identifiers in ways that have produced tremendous efficiencies and benefits for all Americans. For example, our nation's remarkably efficient credit-reporting system relies fundamentally on the Social Security number as a common identifier to compile disparate information from many different sources into a single, reliable credit report. And as set forth in detail in our written statement, the banking, insurance, and securities industries each uses Social Security numbers for a variety of important business transactions, primarily to ensure that the person with whom a financial institution is dealing really is that person.

Here is just a small sample of these uses. It is done to combat fraud and identity theft, to accurately assess underwriting risk, to identify money-laundering activities, to transfer assets to third parties, to comply with deadbeat dad laws, and to locate policyholders to pay insurance proceeds.

This, then, leads me to my second point. Because the use of Social Security numbers as unique identifiers is so integral to our economy, overly broad restrictions on their use could have serious unintended consequences. For example, Social Security numbers are critical for fraud detection. Financial institutions rely on information compiled through Social Security numbers to check for inconsistencies that may suggest the occurrence of fraud or identity theft. Any proposal that unduly restricted the use of Social Security numbers for these purposes would make it easier, not harder, for an individual's identity to be stolen. Similarly, an overly broad prohibition on the sale of Social Security numbers, however well intended, could be construed to restrict such activities as the sale of assets among financial institutions where the assets use Social Security numbers as the basis for account identification.

My third point is that there is no need to further restrict the use of Social Security numbers by financial institutions because of strong new protections imposed by the Gramm-Leach-Bliley Act that take effect on July 1. Each financial institution consumer will have the right to block a financial institution from selling or transferring his or her Social Security number to an unaffiliated third party or the general public. There are exceptions to this general rule for legitimate transfers of these numbers; for example, to protect against fraud. But, in that case the recipient of the number is

prohibited from reusing or redisclosing that number for an unrelated purpose.

Thus, a financial institution consumer is protected with respect to a financial institution's transfer of Social Security numbers, yet legitimate and important uses of these numbers remain permissible. As a result, no additional restrictions on the use of Social Security numbers by financial institutions are warranted.

Thank you, Mr. Chairman. The FSCC welcomes the opportunity to participate in this debate, and we would be happy to work with you and others as discussions on this issue proceed.

[The prepared statement of Mr. Dugan follows:]

Statement of John C. Dugan, Partner, Covington & Burling, on behalf of Financial Services Coordinating Council

My name is John Dugan. I am a partner with the law firm of Covington & Burling, and I am testifying today on behalf of the Financial Services Coordinating Council—or "FSCC"—whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, Investment Company Institute, and Securities Industry Association. The FSCC represents the largest and most diverse group of financial institutions in the country, consisting of thousands of large and small banks, insurance companies, investment companies, and securities firms. Together, these financial institutions provide financial services to virtually every household in the United States.

The FSCC very much appreciates the opportunity to testify before this subcommittee on the use and misuse of social security numbers (or "SSNs"). Our comments focus on the integral role of social security numbers in United States commerce; the many consumer benefits that result from financial institutions' use of these numbers; and the potentially negative effects that could occur if undue restrictions are imposed on such use. While the FSCC recognizes that there have been misuses of social security numbers, we strongly urge that any legislation intended to address this problem be carefully targeted to specifically-identified abuses, such as measures to stop identity theft. We believe it is imperative to avoid restrictions on legitimate and beneficial uses of SSNs.

Our testimony today makes three fundamental points:

- ***First,*** following the lead of the U.S. Government for the last 65 years, businesses' legitimate use of social security numbers as unique identifiers of individuals is now woven into the fabric of commercial transactions throughout the country. The use of these numbers has produced real benefits for American consumers and taxpayers, and has become critically important for a wide range of government agencies, financial institutions, hospitals, blood banks, and many other businesses, both large and small.
- ***Second,*** broad restrictions on the use of social security numbers could have serious unintended consequences, including higher credit costs; increased fraud and identity theft; fundamental and costly changes to internal business operating systems; decreased consumer service; and costly delays in consumer transactions.
- ***Third,*** Congress has recently enacted comprehensive privacy protections under the Gramm-Leach-Bliley Act that, among other things, place stringent restrictions on financial institutions' use and transfer of social security numbers. In light of these provisions, the FSCC strongly believes that further legislative restrictions on financial institutions' use and transfer of social security numbers are unnecessary.

Our testimony also discusses the potentially negative impact of social security number restrictions on financial institutions' legitimate use of public records.

INTEGRAL ROLE OF SOCIAL SECURITY NUMBERS IN U.S. COMMERCIAL ACTIVITIES

As the GAO noted in its February 1999 report,[1] the Social Security Administration created social security numbers 65 years ago as a means to maintain individual earnings records for the purposes of that program. But Congress soon realized the tremendous value to society of a unique identifier that is common to nearly every American. As a result, it began to require federal government use of the SSN as

[1] "Social Security—Government and Commercial Use of the Social Security Number is Widespread," February 1999, GAO/HEHS–99–28.

a common unique identifier for a broad range of wholly unrelated purposes. For example, "a number of federal laws and regulations require the use of the SSN as an individual's identifier to facilitate automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both."[2] These include federal laws applicable to tax reporting, food stamps, Medicaid, Supplemental Security Income, and Child Support Enforcement, among others. Moreover, as the GAO acknowledged, it has repeatedly recommended in numerous reports that the federal government use SSNs as a unique identifier to reduce fraud and abuse in federal benefits programs.[3]

Following the federal government's lead, American businesses not only complied with federal requirements to use SSNs as identifiers for federal laws unrelated to social security, such as income tax reporting. They also realized the powerful consumer benefits to be derived from comparable business use of SSNs as a common unique identifier. Thus, businesses began to use SSNs in a manner similar to the federal government, e.g., to match records with other organizations to carry out data exchanges for such legitimate business purposes as transferring and locating assets, tracking patient care among multiple health care providers, and preventing fraud and identity theft. Many businesses also use SSNs as an efficient unique identifier for such internal activities as identifying income tax filers.

Similarly, the financial services industry has used the SSN for many decades as a unique identifier for a broad range of responsible purposes that benefit consumers and the economy. For example, our nation's remarkably efficient credit reporting system—which has helped make America's affordable and accessible credit the envy of the world—relies fundamentally on the SSN as a common identifier to compile disparate information from many different sources into a single, reliable credit report for a given individual. And as set forth in considerably more detail in Attachment A to this testimony, the banking, insurance, and securities industries each use SSNs as unique identifiers for a variety of important regulatory and business transactions, primarily to ensure that the person with whom a financial institution is dealing really is that person. Set forth below is a very incomplete sample of the many financial institution uses of SSNs that are listed in Attachment A:

- To combat fraud and identity theft;
- To accurately assess underwriting risk;
- To assist in internal benefits tracking;
- To identify money laundering activities;
- To comply with securities law reporting requirements;
- To transfer assets and accounts to third parties;
- To comply with "deadbeat dad" laws;
- To verify appropriate Department of Motor Vehicle records when underwriting auto insurance;
- To obtain verifiable medical information to underwrite life, disability income, and long term care insurance;
- To locate policyholders to pay insurance proceeds;
- To facilitate a multitude of administrative functions.

As noted in the GAO report, "[s]imply stated, the uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes."[4] Put another way, the use of SSNs as common unique identifiers is now woven into the very fabric of both governmental and commercial transactions in this country, and has been so for decades.

In short, the federal government began the use of SSNs for unrelated identification purposes; it required businesses to do the same under certain federal laws; and its use served as an example for businesses, including financial institutions, for over half a century. These uses have produced tremendous efficiencies and benefits for all Americans. The FSCC strongly urges members of Congress to keep such legitimate uses and benefits, including those financial institution uses listed in Attachment A, in the forefront when considering proposals to restrict the use of SSNs.

UNINTENDED CONSEQUENCES OF BROAD RESTRICTIONS ON USE OF SOCIAL SECURITY NUMBERS

As a result of the widespread use of social security numbers for legitimate purposes, the FSCC remains fundamentally concerned about the unintended consequences of legislation that is intended to restrict the abuse of these numbers. Fail-

[2] *Id.* at p.4.
[3] *Id.*
[4] *Id.,* p.2.

ure to carefully target legislation to avoid these unintended consequences risks serious harm to consumers and the smooth operation of the U.S. economy. Let me provide some specific examples:

• *Potential Harm to Consumers.* Financial institutions' use of social security numbers makes it possible for them to provide a level of service to customers that would otherwise not be possible. By using such numbers to verify individual identities, credit bureaus and others can quickly provide financial institutions with accurate credit histories and verification information on people seeking loans, insurance, securities, and other financial products. This in turn permits a financial institution to act swiftly and efficiently on applications or requests related to these products. Use of social security numbers also enables financial institutions to provide more seamless administrative service, e.g., by allowing a life insurer to more easily verify the identity of an individual seeking to change a beneficiary under a life insurance policy. The FSCC's concern is that a broad restriction on the sale or use of social security numbers, however well-intended, could seriously impede the delivery of such important services by driving up processing costs and impairing decision-making.

• *Increased Risk of Fraud and Identity Theft.* Social security numbers are critical for fraud detection. Banks, insurance companies, and securities firms rely on information available from both public and private sources—with embedded social security numbers to ensure correct identification—to check for "inconsistencies" that may suggest the occurrence of fraud or identity theft. The use of these numbers also helps financial institutions verify credit and other information in order to make sound underwriting decisions that minimize losses. The sophisticated processes used for these purposes rely fundamentally on social security numbers as the common unique identifier to assemble accurate and verifiable information for a given individual. Put another way, without a unique common identifier such as a social security number, we believe it would be easier, not harder, for an individual's identity to be stolen. Thus, to reiterate, we believe that Congress should exercise great caution in restricting the use of social security numbers so as not to risk an increase in consumer fraud or identity theft—a result that would be squarely at odds with the intended purpose of such restrictions.[5]

• *Market Disruption.* A prohibition on the sale of social security numbers could be construed to restrict such activities as the sale of assets among financial institutions, or even the sale of the institution itself. This is so because financial institution assets (e.g., mortgage servicing accounts, credit card accounts, and traditional bank accounts) often use social security numbers as the basis for account identification. When it sells such an asset, a financial institution could be viewed as technically "selling" the embedded social security number as well. Thus, legislative efforts that "directly or indirectly" limit the transfer of social security numbers could effectively preclude such plainly legitimate transactions. To address this problem, businesses would need to rework their internal systems completely to eliminate the reliance on such numbers—a massive and needless expense. Accordingly, we believe that any legislative proposal must be crafted to avoid such a significant unintended consequence.

THE PROTECTIONS OF THE GRAMM-LEACH-BLILEY ACT

The FSCC believes there is no need to further restrict the use of social security numbers by financial institutions in light of the strong new social security number restrictions that will apply to such institutions under the Gramm-Leach-Bliley Act ("GLB Act"), which take effect in just over one month. The GLB Act and its implementing regulations treat a financial institution consumer's social security number as protected "nonpublic personal information."[6] As a result, each financial institution consumer has the right to block a financial institution from selling or transferring his or her social security number to a nonaffiliated third party or the general public.

There are exceptions to this general rule for legitimate transfers of social security numbers, such as ones that are necessary to carry out a transaction requested by the consumer; to protect against fraud; to provide necessary identifying information

[5] Existing law already includes provisions that prohibit identity theft. Stealing someone's identity is punishable by civil and criminal penalties under 18 U.S.C. 1028. Moreover, the recently-passed Gramm-Leach-Bliley Act bans pretext calling, which is a basic tool of identity thieves.

[6] *See, e.g.,* 12 C.F.R. § 40.3(o), generally defining protected "personally identifiable financial information" to include "*any* information . . . [t]he bank . . . obtains about a consumer in connection with providing a financial product or service to that consumers" (emphasis added).

to a credit bureaus, etc. However, even with respect to such legitimate transfers of social security numbers, the consumer remains protected because the recipient of the number is prohibited by law from re-using or re-disclosing the number—it may do so only as necessary to carry out the purpose of the exception under which the number was received from the financial institution. Indeed, this unprecedented restriction on the re-use and re-disclosure of consumer information, including social security numbers, was recently upheld by the federal district court of the District of Columbia.[7]

In short, as the result of the GLB Act's carefully-targeted restrictions, a financial institution consumer is fully protected with respect to a financial institution's transfer of social security numbers, yet legitimate and important uses of these numbers remain permissible. In light of these restrictions, no additional restrictions on use of SSNs by financial institutions are warranted.

CONCERNS OVER RESTRICTIONS ON ACCESS TO PUBLIC RECORDS

Finally, some concerns have also been expressed regarding the inappropriate use of social security numbers available in the public record. The FSCC believes it is important to remember that a wide range of private sector enterprises—including banks, insurance companies, and securities firms—rely on such records to conduct a broad range of legitimate business activities. For example, financial institutions use public records to:

- Uncover fraud and identity theft;
- Make sound credit and other financial product determinations;
- Verify identities of the customer at the account opening phase;
- Assist in internal security operations (e.g., employee background checks); and
- Otherwise verify identities in order to conduct a broad range of business transactions.

Business reliance upon such records facilitates the efficient operation of the financial and credit markets, limits mistakes, and ensures that consumers receive prompt and lower-cost service. It also helps protect the customer from fraud.

More specifically, to achieve the purposes described above, financial institutions directly use court bankruptcy records; public records involving liens on real estate; criminal records and fraud detection databases, such as the National Fraud Center database; and similar types of public records. Financial institutions also indirectly use such records for the same purposes by relying on databases developed by third parties that themselves rely on information from public records. Importantly, SSN identifiers are central to ensuring that the information included in these records matches the correct individual. This allows banks, for example, to verify the identity of a person so that a direction from a customer to transfer funds to a third party can be executed without mistake, as well as to check important credit-related characteristics of loan applicants (such as pending bankruptcies, tax liens, or other credit problems).

Moreover, financial institutions employ sophisticated programs that cross-check public information against information supplied by an applicant in order to uncover fraud. For example, if the age information provided by an applicant posing as another individual were inconsistent with other information known about that individual from public records made available through SSN identification, a "red flag" would be raised, which would trigger further checking to uncover the identity theft.

Thus, overly-broad limits on access to public record information would compromise a financial institution's ability to make sound business decisions and protect its customers. Such limits could also greatly slow the decision-making process of U.S. businesses, to the detriment of consumers and the economy.

Finally, even if financial institutions were exempted from restrictions on access to public records containing social security numbers, such restrictions could still create indirect problems for financial institutions and their customers. For example, if a social security number were stricken from a public record, it is possible that the ability to use that record for legitimate purposes would become impossible because of the expense involved in verifying the identity of the person covered by that record. The consequences could be delayed loan approvals, increased consumer costs for products and services, and limits on an institution's ability to discover identity theft on a timely basis.

Even if public entities could still retain social security numbers in their internal nonpublic files, the cost and delays in efficiently accessing such files would be significant. Ultimately, the cost efficiencies and speed of delivery inherent in our cur-

[7] ISRG v. FTC, C.A. No.: 00–1828 (ESH) (Dist. DC, April 30, 2001).

rent market system would be compromised. The effect could be the same as denying financial institutions access to such records.

CONCLUSION

The benefits to society from the legitimate and responsible use of social security numbers are real and substantial. As a result, the FSCC believes that policymakers should look carefully at the unintended consequences that could occur with any proposal that would restrict the use of these numbers. And, because of the GLB Act's imminent restrictions on financial institution disclosure of social security numbers, we believe that no new SSN restrictions are required for the financial services industry. The FSCC welcomes the opportunity to participate in this debate, and would be happy to work with you and others as discussions on this issue proceed.

ATTACHMENT A

ACTIVITIES POTENTIALLY IMPAIRED BY RESTRICTIONS ON SOCIAL SECURITY NUMBERS

As noted above, a wide range of legitimate activities conducted by financial institutions would be affected by broad restrictions on the use of social security numbers. Set forth below are examples of such activities, grouped by the respective industries represented by the FSCC.

I. BANKING INDUSTRY USES

A. General Uses of Social Security Numbers

- *To assist in account administration and better respond to customer requests.* Financial institutions must use shared information to create central databases that then permit institutions to better respond to customer requests or needs (e.g., provide account balances, correct inaccuracies, process loan requests, etc.). To do this, many institutions use social security numbers as a unique identifier to ensure more accurate records.
- *To combat fraud and identity theft.* Financial institutions rely on third-party databases to investigate claims of fraud and identity theft. These third-party databases in turn rely on social security numbers as the common unique identifier that is used by a variety of data sources. Without such common unique identifiers, there would be no way to ensure that particular information is associated with a particular individual, and not with someone posing as that individual. Thus, SSNs are integral mechanisms for accumulating and processing authentic information for both law enforcement officials and financial institutions.
- *To accurately assess risk.* Everyday, financial institutions make judgments regarding financial risks. Institutions must rely on information databases to make such judgments, whether they are decisions on loans, insurance products, or other financial services. Social security numbers, when used by internal and third-party data providers as a means of compiling accurate information on an individual, help institutions make prudent decisions on product offerings.
- *To verify the identity of the customer—in person, over the phone, by mail, or over the internet—in the account opening stage.* A financial institution uses a social security number as the unique individual identifier when verifying information of a person with whom the institution has had no previous contact.
- *To identify potential money laundering activities.* Institutions use social security numbers as unique identifiers to comply with various government requirements, such as Office of Foreign Assets Control (OFAC) verifications or the processing of certain Bank Secrecy Act-related documents (e.g., cash transaction reports).
- *To meet other government safety and soundness requirements.* Federal and State bank regulators require banks and savings associations to operate in a safe and sound manner, and require institutions to develop sophisticated internal policies and procedures to that end. To do so, banks often rely on third-party databases that themselves rely on social security numbers to promote accuracy. As a result, the use of social security numbers plays a significant role in bank internal risk activities.
- *When providing tax reporting information* to the Government (e.g., Forms 1098/1099), as well as to the employee (e.g., W–2s).
- *To facilitate internet banking operations.* Many third-party vendors who provide links to such services rely on social security numbers as account identifiers.

• *To assist in internal security operations.* Institutions use social security numbers as an employee identifier for purposes of background checks and other activities.

• *To assist in internal benefits tracking.* For example, to provide reimbursements to employees incurring business expenses, or to track employee participation in employee retirement funds (e.g., 401(k) plans).

• *To track external payments to vendors for tax reporting purposes.*

• *To permit customer access to a wide range of 24-hour banking services via phone or internet.* Many banks use social security numbers as the account identifier, both as a convenience to customers and to maintain consistency with other internal processing needs, such as the maintenance of an accurate central database and the subsequent ability to use such numbers when making external credit checks.

B. Type of Institutions that Benefit

• *To facilitate financial holding company operations of benefit to the company and its customers.* Holding companies share customer information (including social security numbers) within their corporate family (i.e., affiliates) for a variety of purposes, including:

• *Providing customers with consolidated statements reflecting the status of all of their financial accounts and investments.* To do so, companies need to ensure that customer information matches the correct file—e.g., that the "John Smith" on the phone is the John Smith that has two checking accounts, a variable life insurance policy, and holds the securities of four particular companies. Using social security numbers—the only truly common unique identifier—to verify this information greatly enhances company accuracy and increases customer confidence.

• *Assisting each affiliate in combating identity theft* by giving these affiliates necessary information on the customer so that they may protect the customer's interest. For example, having accurate, up-to-the-minute customer information allows affiliates to quickly identify inconsistencies or irregular activities in a customer's accounts that may reflect that identity theft is occurring. Again, reliance on social security numbers as the "common" element that permits institutions to cross-check existing customer information with new information helps institutions help their customers.

• *Allowing all aspects of the company to prudently manage risk.* When a customer enters a bank, insurance company or securities firm in search of a financial product or service, a financial institution must quickly and accurately gauge its financial risks in providing that product or service. The institution must rely on a variety of credible internal and external databases, such as those provided by credit bureaus, third-party vendors and other affiliates, for accurate information on the credit standing and financial health of the applicant. To ensure that these databases are as accurate as possible, such providers must rely upon some form of common identifier that ensures that correct financial history information is associated with the right person. Social security numbers, as the most accurate common identifier available, help ensure the highest available level of accuracy in these databases. Since a financial institution can then rely on the accuracy of this information in assessing its risk, it can make quick, efficient and prudent decisions regarding the new customer.

C. Securities Industry Uses

• *Account identification.* Many securities firms' systems rely heavily on social security numbers for identification. In general, account relationships are maintained based on SSN as the sole unique identifier for an individual.

• *Tax reporting.* SSNs appear on account opening documentation, primarily for tax reporting purposes.

• *Telephone verification.* Firms use SSNs to verify the identity of a client transacting business over the telephone—this enables firms to access an account by keying in the SSN if the customer does not remember his/her account number.

• *Account searches.* Firms use SSNs for account searches, thus enabling firms to sort all accounts for a customer under the same SSN.

• *Court Actions/Judicial Process/Subpoenas.* Securities firms are often required to provide documents, which would reveal SSNs of a client in responding to a subpoena, court order, or judicial process. Firms also use SSNs to search for accounts in response to requests from regulators and law enforcement officials.

• *Securities law reporting.* Many of the reports securities firms are required to file with the SEC and self regulatory organizations are based on SSN searches and identify SSNs. For example, certain reports to stock exchanges are based on total positions by related party (i.e., SSN).

• *Institutional risk control/anti-fraud.* Firms may use SSNs to perform anti-fraud background checks on potential clients in order to determine whether for example the person has a history of defrauding others.

• *Compliance.* SSNs are used to identify certain types of activity that firms are required to conduct surveillance for, such as excessive turnover in accounts.

• *Communications to shareholders.* SSNs are used in connection with mutual fund mailings, including the mailing of proxy statements and prospectuses to proprietary fund shareholders. SSNs are also used in connection with dissemination of a company's annual report, quarterly report, or interim report.

• Escheatment/Abandoned Property. Securities firms are required to provide on an annual basis to individual States the name, last known address, SSN, and other information for purposes of complying with various State escheatment and abandoned property laws, and intangible property tax laws.

• Transfers of accounts to third parties. SSNs are used to facilitate a customer request to transfer an account to another securities firm, or to satisfy a customer request that a physical stock certificate be transferred from street name into his or her name.

• Insurance. SSNs may also be disclosed where a client purchases an insurance policy through the securities firm—the securities firms would then have to disclose (through the client's application) information, including SSN, to the insurance company.

D. Insurance Industry Uses:

1. Property/Casualty Insurers' Use of Social Security Numbers

• To the extent the p/c insurance industry uses SSNs, that use is confined to legitimate business practices such as underwriting policies, complying with numerous state and federal laws, and verification of identity.

• A proposal to prohibit or limit the disclosure of SSN could restrict p/c insurers from obtaining necessary information for underwriting and verification purposes.

• For example, auto insurers use motor vehicle records to assess insurance risks, reevaluate risks undertaken, conduct claims fraud investigations and pay injured victims. Motor vehicle records, which include social security numbers as identifiers, are an essential source of information needed by insurers to comply with state consumer protection laws and existing contracts.

• Auto insurers may use SSNs obtained from the consumer in order to verify the receipt of proper Department of Motor Vehicle records.

• Undue restrictions on use of SSNs could also impair the ability of p/c insurers to comply with reporting requirements under current federal and state laws, such as those described below.

• Federal laws require p/c insurers to report certain payments with the claimant's SSN to the IRS.

• P/C insurers are required under the Federal Welfare Reform Act to report to state welfare agencies certain information, including SSNs, so that the state can seize settlement dollars from non-custodial parents.

• Under state workers compensation laws, p/c insurers are required to file accident claims (which include the claimant's SSN) with various agencies for those agencies' claims administration purposes.

• States laws require p/c insurers to disclose to state-licensed advisory organizations certain information, which may include a SSN. The state-licensed advisory organizations perform a critical function in insurance pricing by using the information to conduct actuarial projections of anticipated losses so that state insurance regulators are able to perform their duties and insurance companies can establish rates in accordance with state-approved rating systems.

2. Life, Disability Income, and Long Term Care Insurers' Use of Social Security Numbers.

Life, disability income, and long term care insurers are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. However, in order for insurers to serve their prospective and existing customers, they must use and share

nonpublic personal information, including social security numbers, in connection with the origination, administration, and servicing of insurance products and services. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. ACLI member companies also believe that the use and responsible sharing of information generally increases efficiency, reduces costs, and makes it possible to offer economies and innovative products and services to consumers that otherwise would not be available.

(a) Underwriting life, disability income, and long-term care insurance policies—The price of life, disability income, or long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Life, disability income, and long term care insurers gather this information during the underwriting process. Based on this information, the insurer groups insureds into pools in order to share the financial risks presented by dying prematurely, becoming disabled, or needing long term care.

This system of classifying proposed insureds by level of risk is called risk classification. It enables insurers to group together people with similar characteristics and to calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. The process of risk classification provides the fundamental framework for the current private insurance system in the United States. Risk classification is essential to insurers' ability to determine premiums that are adequate to pay future claims, and are fair relative to the risk posed by the proposed insured.

Insurers must be able to obtain and use both medical and nonpublic personal information, including SSNs, in order to underwrite applications for coverage. SSNs are used in a number of different ways in connection with this process:

- *To obtain verifiable medical information.* Insurers sometimes must use proposed insureds' SSNs in order to obtain medical information about them from doctors and hospitals which use SSNs as identification numbers.
- *To obtain drivers' record information.* Insurers sometimes use motor vehicle record information in underwriting. In some states, insurers are required to use SSNs to obtain this information from the motor vehicle department.
- *To obtain credit report information.* Insurers sometimes use information from credit reporting agencies in underwriting, and SSNs are sometimes required to obtain information from consumer reporting agencies.

(b) Performance of Essential Insurance Business Functions

Once life, disability income, or long term care insurance policies are issued, insurers use their customers' personal information to perform essential, core functions associated with insurance contracts, such as for claims evaluations and policy administration. The ability to use this information for these purposes is crucial to insurers' ability to meet their contractual obligations to their customers and to perform important related service and administrative functions. The economies and efficiencies devolving from these functions inure to the benefit of insurers' customers.

Life, disability income, and long term care insurers view SSNs as unique identifiers and use them in a number of ways that enable them to better and more efficiently serve their customers and to protect their interests. They use SSNs to perform a number of these core insurance business functions, which include the following:

- *To locate policyholders.* SSNs are used by insurers to find missing or lost policyholders to inform them that they are entitled to life insurance proceeds.
- *For customer service.* SSNs are used to identify policies owned by an individual who does not have the account or policy number available when a service request is made.
- *For phone call verification.* Insurer call centers use SSNs as part of the data requested to authenticate customers who call with requests for service or for product or account information or status.
- *To transfer assets to unaffiliated financial institutions.* SSNs are often needed to transfer assets from one financial institution to another, for example, for purposes of transfers between mutual funds or annuities and life insurance. (Since one financial institution generally does not know an individual's account number at another financial institution, the SSN is needed to identify the client's identity for the two institutions. This reduces delay, error, and misplaced assets in such transfers.)
- *Pension plan administration.* Insurers also use SSNs in connection with the administration of pension plans, as identification numbers.
- *For online services.* Insurers use SSNs as PIN numbers for customers' use of on-line services.

• *As identification for group insurance plans.* Insurers use SSNs in reporting to employer policyholders under employee group insurance plans and in connection with payroll deductions under these plans.

(c) Disclosures Pursuant to Regulatory/Legal Mandates or to Achieve Certain Public Policy Goals

In furtherance of public policy goals designed to protect American insurance consumers, life, disability income, and long term care insurers share personal health and nonpublic personal information, including SSNs, to:

• *State insurance departments* to assist them in their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers;

• *Self-regulatory organizations,* such as the Insurance Marketplace Standards Association (IMSA), which impose and monitor adherence to requirements with respect to member insurers' conduct in the marketplace; and

• *State insurance guaranty funds,* which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information.

Any limitation on these disclosures would seem likely to operate counter to the underlying public policy reasons for which they were originally mandated—to protect consumers.

Life, disability income, and long term care insurers are also required to make certain disclosures of information by the federal government. In addition, they need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies and state insurance departments. Their primary purpose is to reduce the cost of insurance by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. Any limitation on insurers' right to make these disclosures would seem likely to undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.

Life, disability income, and long term care are required to use SSNs to report to the IRS a variety of payments to insurance consumers, including, but not limited to, interest payments, certain dividends, and policy withdrawals and surrenders. At least one state, Rhode Island, requires that insurers match "deadbeat" parents data before making payments on claims. SSNs are required for that matching.

(d) Ordinary Business Transactions

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Naturally, these files can contain personal information, including customers' SSNs. Such disclosures are often necessary to the due diligence process that takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly-created entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements often necessitate the disclosure of personal information, which may include SSNs, by the primary insurer to the reinsurer.

Mr. COLLINS. Thank you, Mr. Dugan. Mr. Rotenberg?

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, AND ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman, and members of the Committee. I am both executive director of the Electronic Privacy Information Center and on the faculty at Georgetown Law Center where I have taught privacy law for the last 10 years. I have also participated in two of the leading Social Security number cases, and I would like to fill in a bit of the background on the legal history for this issue to give you some sense

of Congress's authority to act to regulate the misuse of the Social Security number.

As Mr. Hendricks described earlier, an important report in 1973 on record keeping practices across both the Federal Government and the private sector recommended restrictions on the use of the SSN. One of the key recommendations of the report in 1973 was prohibiting the use of the Social Security number or any number represented as an SSN for promotional or commercial purposes.

Now in 1974 with the passage of the Privacy Act, Congress did not act on the recommendation to regulate the use of the SSN in the private sector. It did, however, regulate the use of the SSN by Federal agencies. And an important provision in the Privacy Act, Section 7, set out a series of safeguards in an effort to ensure that the SSN would not be too widely used by the Federal Government.

Now, as several of the witnesses have testified earlier, the use of the SSN has expanded significantly over the last 25 years but this has been particularly true in the financial services sector and that is what has given rise to growing concerns about identity theft.

I would like to say a few words about the cases that I participated in regarding the use of the SSN because I think they speak to the critical issue here and the privacy interest that underlies Congress's efforts to regulate in this area, as well as the court's recognition that it is appropriate to regulate in this area.

In 1992 I filed a brief in support of a registered voter in the State of Virginia, Mark Greidinger, who was asked to provide his Social Security number as a condition of his right to vote in that State. He objected to the fact that he was asked for his SSN because the State of Virginia at that time not only collected the SSN but they also published it in the voting roll, effectively a public record and making it freely available for others to use for whatever purposes they wished.

We argued that this was an unreasonable burden on the right to vote. The Fourth Circuit agreed and this is what they had to say: "Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards or even obtain the person's paycheck. Succinctly stated, the harm that can be inflicted from the disclosure of an SSN to an unscrupulous individual is alarming and potentially financially ruinous." I think there was a great deal of prescience in this opinion from the court more than eight years ago.

In a second case testing whether a State could be required to disclose the Social Security number of a State employee under a State open record law where there was a strong presumption in favor of disclosure, the Ohio Supreme Court held that there were privacy limitations in the Constitution that weighed against disclosure of the SSN. The court said in that case, "We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information

about government processes gained through the release of the SSNs."

In both of these cases courts have made clear the importance of restricting the use of the Social Security number and drew particular attention to the potential financial consequences of the misuse of this information.

Now the question has been raised recently whether it is possible that the First Amendment limits the ability of Congress to legislate in this area. I think based on the two recent opinions in TransUnion versus FTC and in IRSG versus FTC, the courts have made clear that it is appropriate to legislate to protect privacy where there is a substantial interest in that outcome.

Finally, I would like to say just a few words about the form of the legislation that we think the committee should adopt at this point in time. We think the best guiding principle is to try to limit the use of the Social Security number to those circumstances where use is explicitly authorized by law. So, for example, if an employer needs an SSN for tax reporting purposes or if a bank needs an SSN for the purpose of identifying an interest-bearing account, I do not think there could be any objection to the collection and use of SSNs in those circumstances.

But the types of open-ended uses, which I think were very well described by Mr. Kravit earlier, that students and consumers and many people today across America face for transactions totally unrelated to tax-reporting purposes, could quite appropriately be limited.

There are other recommendations in my statement for the Committee and I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

Statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, and Adjunct Professor, Georgetown University Law Center

My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information Center, a public interest research organization based here in Washington DC. I am also on the faculty of the Georgetown University Law Center where I have taught the Law of Information Privacy for ten years. I have also participated in the litigation of two of the leading cases on the use of the Social Security Number.

I appreciate the opportunity to testify this morning. I will briefly review the legal status of efforts to regulate the use of the SSN, discuss some of the recent problems with universal unique identifiers, such as the SSN, and make a few brief recommendations. I believe that legislation to limit the collection and use of the SSN is appropriate, necessary, and fully consistent with US law. I also believe that if Congress fails to act, the problems that consumers will face in the next few years are likely to increase significantly.

I should note also that the Supreme Court just yesterday issued a ruling in an important case concerning a First Amendment challenge to the publication of information obtained by means of illegal wiretap. I will say a few words about the possible significance of this opinion for SSN legislation under consideration now by Congress.

History of the SSN and the Efforts to Regulate

The Social Security Number (SSN) was created in 1936 as a nine-digit account number assigned by the Secretary of Health and Human Services for the purpose of administering the Social Security laws. SSNs were first intended for use exclusively by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs were permitted to be used for purposes unrelated to the administration

of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.[1]

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security Number that show a striking resemblance to the problems that consumers face today. Although the term "identity theft" was not yet in use, Records Computers and the Rights of Citizens described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."[2]

In response to growing concerns over the accumulation of massive amounts of personal information and the recommendations contained in the 1973 report, Congress passed the Privacy Act of 1974. Among other things, this Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. This is a critical principle to keep in mind today because consumers in the commercial sphere often face the choice of giving up their privacy, their SSN, to obtain a service or product. The drafters of the 1974 law tried to prevent citizens from facing such unfair choices, particularly in the context of government services. But there is no reason that this principle could not apply equally to the private sector, and that was clearly the intent of the authors of the 1973 report.

In addition, Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it.[3] At the time of its enactment, Congress recognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation."[4] Short of prohibiting the use of the SSN outright, this provision in the Privacy Act attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed where the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

The use of the SSN has expanded significantly since the provision was adopted in 1974. This is particularly clear in the financial services sector. In an effort to collect and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs, and it is these companies that are among the strongest opponents of SSN restrictions. For example, credit bureaus maintain over 400 million files, with information on almost ninety percent of the American adult population. These credit bureau records are keyed to the individual SSN. Such information is freely sold and traded, virtually without legal limitations.[5]

But it is also critical to understand that the legal protection to limit the collection and use of the SSN is still present in the Privacy Act and can be found also in court decisions, which recognize that there is a constitutional basis to limit the collection and use of the Social Security Number. When a Federal Appeals court was asked

---

[1] Pub. L. No. 87-397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676) cited in Greidinger at 27-28.

[2] Records, Computers and the Rights of Citizens at 135.

[3] (a)(1) It shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (2) the provisions of paragraph (1) of this subsection shall not apply with respect to—(A) any disclosure which is required by Federal statute, or (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

See Pub. L. No. 93-579, 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A 552a (West 1996).

[4] S. Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943, cited in Greidinger at 29.

[5] Komuves at 557.

to consider whether the state of Virginia could compel a voter to disclose an SSN that would subsequently be published in the public voting rolls, the Court noted the growing concern about the use and misuse of the SSN, particularly with regard to financial services. The Fourth Circuit said:

> Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck. . . . Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous.[6]

The Court said that:

> The statutes at issue compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote. As illustrated by the examples of the potential harm that the dissemination of an individual's SSN can inflict, Greidinger's decision not to provide his SSN is eminently reasonable. In other words, Greidinger's fundamental right to vote is substantially burdened to the extent the statutes at issue permit the public disclosure of his SSN.[7]

The Court concluded that to the extent the Virginia voting laws, "permit the public disclosure of Greidinger's SSN as a condition of his right to vote, it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments."[8]

In a second case, testing whether a state could be required to disclose the SSNs of state employees under a state open record law where there was a strong presumption in favor of disclosure, the Ohio Supreme Court held that there were privacy limitations in the federal Constitution that weighed against disclosure of the SSN. The court concluded that:

> We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs. Our holding is not intended to interfere with meritorious investigations conducted by the press, but instead is intended to preserve one of the fundamental principles of American constitutional law—ours is a government of limited power. We conclude that the United States Constitution forbids disclosure under the circumstances of this case. Therefore, reconciling federal constitutional law with Ohio's Public Records Act, we conclude that [the provision] does not mandate that the city of Akron discloses the SSNs of all of its employees upon demand.[9]

While it is true that many companies and government agencies today use the Social Security Number indiscriminately as a form of identification, it is also clear from the 1936 Act, the 1974 provision, and these two cases—Greidinger v. Davis and Beacon Journal v. City of Akron—that there is plenty of legislative and judicial support for limitations on the collection and use of the SSN. The question is therefore squarely presented whether the Congress will at this point in time follow in this tradition, respond to growing public concern, and establish the safeguards that are necessary to ensure that the problems associated with the use of the SSN do not increase.

More recently, the question has been raised whether the First Amendment could limit the ability of Congress to pass legislation protecting personal information. But two different courts in the context of the privacy provisions contained in the Financial Services Modernization Act have made clear that such statutes are permissible.

In TransUnion v. FTC the DC Circuit found that the government's interest in keeping personally identifiable information private was substantial and upheld the FTC's ban on the sale of target marketing lists. And a DC District Court in IRSG v. FTC upheld restrictions on "credit header" information, which includes names, address, and social security number, and said that:

> The speech does not involve any matter of public concern, but consists of information of interest solely to the speaker and the client audience. Thus, restriction on the dissemination of this nonpublic personal information does not impinge upon any public debate.

Id. at 51.

---

[6] Greidinger at 30-31.
[7] Greidinger at 32-33.
[8] Greidinger at 36.
[9] Beacon Journal at 17.

In some circumstances, for example when the SSN is used in the context of political speech, then the privacy interest would likely give way to the First Amendment interest. If, for example, a journalist or a political activist were to disclose an SSN for the purpose of drawing attention to a privacy issue, then I believe a court must review any effort to restrict such speech under strict scrutiny analysis. But where the SSN is collected, used, and disclosed in the context of commercial relations, then I believe a privacy statute would survive a Constitutional challenge.

Specific Problems with the IRSG

Several years ago significant public concern was raised about information brokers that routinely buy and sell detailed personal information, including Social Security Numbers. The Individual Reference Services Group was established to improve practices in the industry. We do not believe these principles provide sufficient safeguards for consumers. We also do not think the discussion between public and non-public information incorporated in GLB is consistent with the general purpose of privacy laws.

IRSG companies gather and sell Social Security numbers. Social Security numbers are collected from a variety of public and non-public sources. Public documents such as bankruptcy filings and other types of court records often contain Social Security numbers of the parties to a proceeding. Non-public documents such as credit headers, the identifying information at the top of credit reports (including names, addresses, ages and SSNs), are also culled for information. IRSG companies use both public and non-public sources of personal information to compile data on individuals.

During 1997, the IRSG worked with the Federal Trade Commission, absent public input, to develop a set of self-regulatory principles.[10] These self-regulatory principles allow the sale of Social Security numbers without the knowledge and permission of the data subject.

Under the IRSG Principles, companies can freely sell and distribute SSNs gathered from public records. The IRSG Principles treat the same data, Social Security numbers, differently if it comes from a non-public source such as credit headers. However, the guidelines for the sale of Social Security numbers from non-public sources are completely subjective and largely ignore the privacy interests of the data subject.

The IRSG Principles create a three-tier system for the sale of information gathered from non-public sources. The first tier for the sale of Social Security numbers applies to "qualified subscribers." Complete Social Security numbers can be sold to those deemed to fall into this category. There is no definition of what makes someone whom wishes to purchase a social security number a "qualified subscriber." Moreover, the conditions that qualified subscribers must meet under the IRSG Principles rely entirely on the determination of the data seller and the data purchaser on what is an "appropriate" use of such information. The data subject, the person whose Social Security number is being collected and sold, has no input into whether such use is in fact "appropriate."[11] The balancing process for deciding whether such uses are appropriate is carried out by the parties selling and purchasing the data; that is, the ones that have a strong interest in letting a transaction proceed. In addition, IRSG companies do not have a strong incentive to establish whether information being sold to a responsible entity that will use data in a strictly appropriate manner.

Oversight of IRSG companies is generally weak. Yearly assessments required by the IRSG Principles, are conducted by "reasonably qualified independent professional" services. The assessment criteria, in many places, simply ask whether IRSG companies have some process in place, rather than evaluating whether such a process is effective.[12] The assessment criteria do not seek to evaluate whether such qualifications are stringent enough or even if they are evenly applied among different IRSG companies. The criteria do not even try to offer some metric against which qualifications can be measured. In addition, none of the results of assessments are publicly displayed. None of the third-party assessments conducted in the past three years provide the answers to the questions asked during the assess-

[10] http://www.irsg.org/html/industry_principles_principles.htm

[11] The terms appropriate or appropriately are defined as "actions or uses that are reasonable under the circumstances reflecting a balance between the interest of individual privacy and legitimate business, governmental, and personal uses of information, including prevention and detection of fraud."

[12] http://www.irsg.org/html/criteria.htm

ments.[13] The third-party assessment information page simply lists the company that conducted the assessment.

The failings of the IRSG Principles, and their general disregard of privacy protections, are a result of the lack of statutory protections for the underlying information. Without such legal protection for personal information, companies like the members of the IRSG will continue to traffic in personal data without the knowledge or permission of data subjects.

Crafting SSN legislation

We believe it is appropriate, necessary and consistent with other privacy measures to develop and enact legislation in the 107th Congress that will safeguard the use of the SSN. We also believe it is important to take a long-term view of the SSN. The best legislative strategy is one that discourages the collection of the SSN and that encourages organizations to develop alternative systems of record identification.

We further recommend that legislation:

- Limit the use of the SSN to those circumstances where use is explicitly authorized by law. For example, an employer should be permitted to ask an employee for an SSN for tax-reporting purposes (as long as the SSN remains the Taxpayer Identification Number), but a health club should not be permitted to ask a customer for an SSN as a condition of membership.
- Prohibit the sale and limit the display of the SSN by government agencies. It is simply inconsistent with Section 7 of the Privacy Act to allow the federal government to disseminate the SSN.
- Prevent companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request
- Penalize the fraudulent use of another person's SSN but not the use of an SSN that is not associated with an actual individual. This would permit, for example, a person to provide a number such as "123-00-6789" where there is no intent to commit fraud.
- Encourage the development of alternative, less intrusive means of identification. We believe that the National Research Council should be funded to undertake research on new techniques that enable records management while minimizing privacy risks.

We do not believe there is any reason to distinguish between Internet-based and non-Internet based disclosure of SSN. The legislation in this area should focus on the subject matter and remain "technologically neutral." We also favor a proposal made by Robert Ellis Smith, publisher of the Privacy Journal, that would prohibit the sale or purchase of an SSN.

Conclusion

It is important to emphasize the unique status of the Social Security Number in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy. Given the unique status of the SSN, the established link to identity theft and the specific economic harms that result, as well as the clear history in federal statute and case law, it is fully appropriate for Congress to pass legislation.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

REFERENCES

Electronic Privacy Information Center, "Social Security Numbers" [http://www.epic.org/privacy/ssn/]

Flavio L. Komuves, "A Perspective on Privacy, Information Technology and the Internet: We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," 16 J. Marshall J. Computer & Info. L. 529 (1998)

Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "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)

Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN requirement for voter registration) (lead case on privacy of Social Security number)

[13] http://www.irsg.org/html/3rd__party__assessments.htm

Beacon Journal v. City of Akron, 70 Ohio St. 3d 605 (Ohio 1994) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN disclosure of city employees)

IRSG v. FTC, Memorandum Opinion, D.C. Cir., Apr. 30, 2001.

Marc Rotenberg, Privacy Law Sourcebook: United States Law, International Law, and Recent Developments (EPIC 2000)

Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens 108–35 (MIT 1973) (Social Security Number as a Standard Universal Identifier and Recommendations Regarding Use of Social Security Number)

Mr. COLLINS. Thank you, sir. Mr. Plesser?

STATEMENT OF RONALD L. PLESSER, PARTNER, PIPER MARBURY RUDNICK & WOLFE LLP, AND COORDINATOR, INDIVIDUAL REFERENCE SERVICES GROUP

Mr. PLESSER. Thank you. My name is Ron Plesser and I will speak quickly. With me is Paula LeRoy, who is president of Pension Benefit Information Services from California and Mrs. LeRoy, I think, has some very interesting and important uses of Social Security numbers.

I would like to make several very quick points. I am the coordinator of the Individual Reference Services Group, which is a group of 14 companies that came together five years ago to try to create a self-regulatory environment with the approval of the Federal Trade Commission to limit some of the abuses of Social Security numbers and to put on industry some controls.

We think it has worked well but we have also supported legislation, particularly legislation that would prohibit the use of the Social Security number on the Net. Our rules prohibit the use of disclosure to the public and the kind of demonstrations we saw today were ones that would certainly have been outside and in violation of our rules and we would support legislation.

We think display should be limited to the public but it should allow for broad benefits to allow legitimate business uses. We can notice from the testimony this morning all of the awful cases of identity theft that we heard all had the word "theft" in it. All had theft of a gym bag, theft by a waiter, theft of somebody who worked in an HMO. I think we have to focus on what the real problems are, which are people actually stealing information, not legitimate business purposes.

I would like to go through very quickly, in addition to Mrs. LeRoy's example, it is used indeed for missing children. It is used for locating witnesses. The information is used by law enforcement when they want to identify people.

And I think I would like to make one final point, that the uses of lists of individuals with the names and addresses and Social Security numbers for business purposes allows identity theft to be decreased. If a bill prohibiting those uses are passed it would be my sense and I think I agree with my colleague here that identity theft would increase. I do not think there is very much question about that and I think that has to be looked at.

We look very much forward to working with the Committee on legitimate purposes and going forward and working with you on the legislative process.

[The prepared statement of Mr. Plesser follows:]

Statement of Ronald L. Plesser, Partner, Piper Marbury Rudnick & Wolfe LLP, and Coordinator, Individual Reference Services Group

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it examines the issues of protecting privacy and preventing misuse of social security numbers. My name is Ronald Plesser and I am the coordinator of the Individual Reference Services Group (IRSG). The IRSG is a group of the leading information industry companies, including major credit reporting agencies, that provide services to help identify, verify identity of, or locate individuals. Since 1997, member companies have followed self-regulatory principles to respect consumer privacy. These principles were developed in 1997 in conjunction with the Federal Trade Commission.

The members of the IRSG are committed to the responsible acquisition and use of personally identifiable information in business-to-business transactions. We strive to respect consumer privacy as we provide services to the government and businesses. We do not oppose a prohibition of the public display of Social Security Numbers (SSNs) to the public. We share the Committee's concern about the potential misuse of SSNs for identity theft and other harmful purposes. Indeed, in the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential.

My remarks today will focus on three areas. First, because most people know relatively little about our industry, I will explain the customer base and socially beneficial uses for individual reference information. Second, I will provide some background about the IRSG principles and their enforcement mechanisms to demonstrate the effectiveness of the IRSG approach to privacy protection. Finally, I will discuss the IRSG's support of legislative efforts to prevent SSN abuse, and the importance of ensuring that any legislation concerning SSNs preserves the use of SSNs to match records or allow retrieval of location information for an individual by searchers who already know that SSN. We do oppose legislation that would prohibit the purchase and sale of SSNs for legitimate business purposes.

II. Uses of Individual Reference Service Information

Individual reference services are companies that furnish timely and reliable information to identify and locate individuals. The information is used by governmental, private sector, and non-profit entities for a wide range of beneficial purposes. Use of individual reference services often is the only way that individuals with limited resources, through the assistance of a professional who has access to these services, can obtain critical information. IRSG customers are professionals, primarily in the fields of law, business, journalism, and law enforcement.

For example, law enforcement agencies use these services to locate criminals and witnesses to crimes, and to confirm identities. In fact, individual reference services play an important role in combating the very sorts of fraud that flow from personal financial information falling into the wrong hands. At the June 1997 FTC workshop examining reference services, witnesses from both the U.S. Department of Treasury's Financial Crimes Enforcement Network (FINCEN) and the Financial Crimes Section of the U.S. Secret Service testified to the value and importance of these services for their work.

In the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential. Banks, credit card companies, and other types of credit institutions, as well as gas, electric, and telephone companies and governmental entities distributing funds in conjunction with public entitlement programs, are all becoming increasingly plagued by fraudsters who use an existing person's identity to illegally obtain products, services and money. The best, and perhaps only, means of preventing this type of fraud is to crosscheck through the use of personal identifying data, often provided by individual reference services. Since the victims of identity theft are not only the businesses that lose billions to various forms of identity theft per year, but also the consumers whose credit is often ruined by this insidious act, everyone directly benefits by this application of the personal identifying information provided by individual reference services.

Individual reference service products also are an important tool for other types of fraud prevention efforts by businesses. The insurance industry, for example, relies on individual reference service products to investigate fraudulent claims. Credit card companies and department stores use them to detect and limit credit card fraud. Banks use them to detect and report credit card fraud, insider abuse, and money laundering. Many businesses use them to minimize the risk of financial

fraud when they receive an unusual order for delivery of merchandise. Other businesses use them when performing due diligence before engaging in a business venture with a little-known corporation in the increasingly mobile world economy. The Insurance Information Institute reports that special investigation units save their companies about $10 for every dollar invested in them.

Reference services help people in many other ways. One of the most compelling is child support enforcement. Whereas government-compiled child support databases have encountered difficulties in some instances, individual reference services have proven to be invaluable in tracking down parents who are delinquent in these obligations. In this way, these services advance personal responsibility, give much-needed income to divorced parents and their children, help free families from welfare dependency, and provide an additional source of revenue to state welfare programs. Individual reference services can locate non-custodial parents quickly and inexpensively, even in circumstances where they move to a different state or begin using a different name. The Association for Children for Enforcement of Support ("ACES"), the leading child support advocacy organization, uses LEXIS–NEXIS' P–TRAK service to assist families—approximately 80 percent of whom are on welfare—in locating parents who have failed to meet legal child support obligations. ACES has reported tremendous success with this service, locating more than 75 percent of the "deadbeat" parents they sought, and helping families receive much-needed support.

Among the many other important uses of individual reference services are:

- locating pension fund beneficiaries who have left a company,
- finding long-lost family members and missing children,
- locating heirs to estates who have moved or changed their names through marriage,
- locating victims of fraud schemes
- notifying former residents of areas determined to contain environmental hazards,
- protecting consumers from unlicensed professionals and sham businesses,
- locating blood, organ and bone marrow donors,
- promoting the transparency of the political process by providing easy-to-search information on individuals' campaign donations,
- locating witnesses, and
- providing citizens with efficient, ready access to federal, state, and local government information.

These examples reflect the positive benefits that can be derived from careful use of SSNs.

III. The IRSG Approach

Privacy Protection

Rapid advances in technology, a highly mobile society, the need to prevent fraud, and other market demands for information have spurred increased reliance upon information services provided by individual reference service companies. These changes in society and technology also have resulted in a heightened interest in the privacy considerations implicated by such services. The IRSG members have taken a leadership role in effectively addressing privacy concerns.

The IRSG Principles

The importance of defining privacy practices tailored to specific types of information is demonstrated in the IRSG principles.

In September 1996, in the closing days of the 104th Congress, the Federal Trade Commission proposed a broad prohibition on the use of credit header information—non-financial identifying information obtained from a consumer reporting agency's database. Members of the individual reference service industry and those who rely on credit header information alerted Congress that such a prohibition would severely limit important uses of this information. As a result of arguments made by industry, regulatory efforts were postponed until a further study of the issues could be conducted.

Fourteen of the leading companies in the individual reference services industry joined together to form the IRSG. The companies that comprise the IRSG provide information and assist users in identifying and locating individuals. In close consultation with the Federal Trade Commission, the IRSG developed a comprehensive set of self-regulatory principles backed by third-party assessments and government enforcement that these companies follow.

These principles focus on non-public information, that is, information about an individual that is of a private nature and neither available to the general public nor

obtained from a public record. For example, the principles govern information obtained from credit headers, such as SSNs and addresses and telephone numbers.

Companies that sign on to the IRSG principles commit—among other things—to:

- acquire individually identifiable information only from sources known as reputable,
- restrict their distribution of non-public information through appropriate safeguards,
- educate the public about their database services, and
- furnish individuals with a copy of the information contained in services and products that specifically identifies them, unless the information is publicly available.

One of the key safeguards on the distribution of non-public information is a prohibition on the display of SSNs and dates of birth in individual reference service products distributed to the general public and, for products distributed to professional or commercial users, a prohibition on the display of such information unless truncated in an appropriate manner (e.g., masking of the last four or more digits of SSNs). Our companies do not sell SSNs on the Internet, and we do not oppose such a prohibition. Indeed, we have worked hard to prevent SSNs from being sold on the Internet.

Self-Regulation with "Teeth"

Third-party assessments backed by government enforcement provide real "teeth" for enforcing these principles. Enforcement rests on the following three pillars:

- Legal sanctions—Any company that holds itself out to the public as following the principles may be responsible under existing federal and state law if the company fails to live up to them. Both the Federal Trade Commission and state attorneys general can bring charges under Section 5 of the Federal Trade Commission Act and similar state laws against member companies that fail to adhere the principles.
- Cut-off of data supply—Signatories to these principles require by contract that all companies buying non-public data from them for resale abide by the principles. Non-complying companies risk losing access to the data they need for their products or services. This is particularly significant in that the FTC estimated that IRSG signatories control 90% of all non-public information obtained from credit headers.
- Independent assurance reviews—Every IRSG company must undergo an annual third-party assessment to verify compliance with the principles. I describe this in more detail below.

Information Practices

In the spirit of openness, the principles require individual reference services to have an information practices policy statement available to the public upon request. These statements describe:

- the types of information included,
- the types of sources from which that information is obtained,
- the nature of how the information is collected,
- the type of entities to whom the information may be disclosed, and
- the type of uses to which the information may be put.

This openness enables individuals to understand the reference service's use of the information it possesses. Individual reference services also inform individuals, upon request, of the choices available to limit access to or use of information about them contained in a company's products and services. Further, the principles require an individual reference service to provide information about the nature of public record and publicly available information that it makes available in its products and services and the sources of such information.

Third-Party Assessments

To help ensure that member companies do not make unsubstantiated assertions of compliance, the IRSG principles require that independent professional services conduct annual third-party assessments of their compliance. These independent professional services can be accounting firms, law firms, or security consultants who use the criteria developed by PriceWaterhouseCoopers for the IRSG.

When the principles were adopted in December 1997, these companies agreed that the first assurance reviews would be completed within 15 months. I am pleased to report that this is the third consecutive year in which the companies that offer products that fall within the scope of the IRSG principles and subscribe to the principles have successfully undergone these assessments. As this milestone attests, the IRSG has made great strides through self-regulation to secure the benefits of information service resources while ensuring effective protection of consumer privacy.

IV. The IRSG Supports Legislative Efforts to Address SSN Abuse

In addition to the internal measures that we have taken to protect consumer privacy and ensure responsible use of information, including SSNs, the IRSG has supported efforts by some Members of Congress that strike the right balance on SSN privacy. For example, the IRSG supported legislation last year to prevent the public display of SSNs on the Internet. In addition, we supported legislation to prohibit pretext calling. We also have supported legislation to prohibit the purchase, sale, or use of SSNs for illegal purposes, including legislation to prevent individuals from obtaining SSNs for identity theft purposes.

We believe that efforts that focus upon restricting the display or sale of SSNs to the public rather than any sale of SSNs strike the right balance. This approach prevents people from discovering anyone's SSN from a commercial source, thereby protecting privacy. At the same time, it preserves the ability of people who already know someone's SSN, typically in a commercial, governmental, or law enforcement context, to use a commercial database for beneficial purposes.

We would oppose legislation that would ban the purchase and sale of SSNs by businesses who have legitimate business purposes to use the number. Enactment of such legislation would not allow for the continued use of SSNs for indexing and verification of information that is critical to ensuring that the products that the IRSG members offer to professional and governmental agencies contain accurate and complete information. The inability to use SSNs for indexing and verification would, ironically, result in more rather than less identity theft and undermine many of the positive uses outlined above.

V. Conclusion

Members of the IRSG are committed to the responsible acquisition and use of personally identifiable information, and share the Subcommittee's concern about the potential abuse of SSNs. Nevertheless, individual reference service products are absolutely essential to all of the positive and socially beneficial uses outlined above. Congress should not take any steps that would jeopardize the usefulness of such services. We look forward to working with you on this important issue.

Mr. COLLINS. Ms. LeRoy?

STATEMENT OF PAULA LEROY, PRESIDENT, PENSION BENEFIT INFORMATION, TIBURON, CALIFORNIA

Ms. LEROY. Thank you. It is my pleasure to appear before the Subcommittee today as you examine privacy and Social Security numbers.

My name is Paula LeRoy. I am president of Pension Benefit Information, a company located in California. We provide a service that uses Social Security numbers to locate former employees and beneficiaries to ensure that they receive their retirement benefits. We represent approximately 2,500 to 3,000 of the largest pension plans and we locate former employees on behalf of these plan sponsors and benefit administrators.

Often our services are required by law, as in the case of the Pension Benefit Guaranty Corporation (PBGC) accepting assets for a terminating plan. You must use a locating service to try to find all the people first. More often, our services are used for companies and plans who need to do lump sum pay-outs to former employees. Every year we locate over 200,000 individuals who have benefits that they often leave behind and forget about. We locate them and the monetary value is several hundred million dollars returned to individuals.

To find these individuals we are given two pieces of information from the companies: the name and the Social Security number. The

last known address does not work because generally the people are mobile. They leave a job and they move.

When we are given an SSN we search for a current address in one of the commercial databases. If we find several addresses for the individual we mail each address a letter explaining their benefits and what they have due to them and at that time they have the option to respond to our letter and ask for us to put them in touch once again with the employer.

One of the most serious difficulties we have is with women whose names change, so even a name given to us does not work because their names change through marriage.

Continued access to Social Security numbers is critical to this positive use. Searching with the Social Security number we have a success rate of 85 to 90 percent of the people found and put in touch with the employer. Without the Social Security number, the results are dramatically decreased and I fear as we go forward the results will be disastrous.

Any legislation that Congress passes on SSNs should take into account the positive uses, as I just explained, and allow for Social Security numbers to be purchased with addresses. Thank you. I appreciate your interest.

[The prepared statement of Ms. LeRoy follows:]

Statement of Paula LeRoy, President, Pension Benefit Information, Tiburon, California

Good morning Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it examines the privacy and use of Social Security Numbers ("SSN") in both the public and private sectors. I am Paula LeRoy, President of Pension Benefit Information, a company that provides a service that works to ensure that former employees, who are owed retirement benefits, receive them.

Our pension plan clients would be severely impacted by the enactment of legislation that would restrict the purchase and sale of SSNs for matching, search, and retrieval purposes. Such legislative restrictions would have serious consequences for millions of Americans who have earned benefits for their years of employment. We, thus, urge that you oppose any legislation that would restrict the purchase or sale of SSNs to match records or allow retrieval of location information for an individual by searchers who already know the SSN and have a legitimate business purpose.

Pension Benefit Information represents approximately 2,500 pension plans in the United States. We locate missing pension plan participants on behalf of pension plan sponsors and benefit administrators. In the course of administering these pension plans, it is mandated that important plan information, plan changes, and account balances be communicated to all participants, whether they work for the company, or have left employment and moved away. Also, by law, pension fund administrators and sponsors are required, in the case of terminated plans, to conduct a diligent search for missing participants before information about the participant or payment is submitted to the Pension Benefit Guaranty Corporation (PBGC). Under the law, a search is considered diligent if it "includes use of a commercial location service to search for the missing participant. . . ." 29 C.F.R. § 4050.4(b)(3).

Every year, we locate over 200,000 individuals who have retirement benefits due and owing to them. To find these individuals, companies provide us with plan participants' names and SSNs, but in some cases companies are able to only provide us with beneficiaries' names and addresses. In those cases where we are given SSNs, we search for an individual's current address in commercial databases, such as those offered by IRSG members, by typing in the individual's social security number. If several addresses are found during this search, we conduct further research to find the most current address for an individual. We have had tremendous success in using SSNs in these search databases to locate, notify, and provide participants or pension fund beneficiaries with pension plan contact information so that they may obtain pension benefits due and owing to them.

My role here truly is to set forth the positive uses of SSNs. We believe that our business is a prime example of how the use of SSNs yields socially beneficial results. Many of the people we help are older Americans, who desperately need their pen-

sion benefits, no matter how small or large. With so many people changing jobs today, the task of locating former employees is becoming increasingly difficult. Americans move on average every five years, particularly when they change jobs. They also often change their names with marriage or list slightly different names (i.e., leave out a middle initial) on employment documents. These services are, by far, the most cost-effective and efficient way to find these former workers.

The Department of Labor is well aware that billions of dollars in vested pension benefits go unclaimed because people leave an employer and are never advised that they have a benefit due to them at a future date. In some cases, pension fund beneficiaries never receive this income because their current address is unknown to the pension fund trustee or administrator. Although it may have been years since a company employed a beneficiary, personnel records provide the employee's SSN. The SSN can then be used to track this individual in the database.

Our services have been used successfully by numerous employers across America to locate individuals entitled to retirement benefits. On a weekly basis we serve the Fortune 500, as well as the major labor unions, and state governments. One of the most recurring corporate events that contribute to lost participants is mergers and acquisitions ("M & A"). When an M & A activity takes place, the pension assets move to the new company, often in a different city, with a new corporate name. Individuals lose track of these occurrences and, thus, have obvious difficulties tracking down their vested benefits. It is in these situations that employers turn to us for the notification process. For one aerospace contractor, we located 55,000 former employees to give them the information they needed regarding the change in their benefit center information.

Sometimes we locate individuals whose lives are changed dramatically by our use of SSN searches. For example, we were able to track down an estranged wife of a bank executive who had had no contact with her former husband for several years. The woman had been forced to move in with her daughter and had virtually no possessions. Because we knew her SSN and were able to search by using her SSN in a commercial database, we were able to locate her and provide her with pension benefits that she greatly needed.

Similarly, we were able to find a 73-year-old former General Motors employee from Mississippi to notify him of his lost pension, because we knew his SSN and used it to search for his current address in a commercial database. He was entitled to receive these benefits at age 65, but he had never before received notice of this entitlement. This gentleman was awarded his pension once we found him, and he now receives a monthly benefit that he would otherwise never have received, even after 20 years of service to General Motors. Once he started to receive his much-welcomed benefits, he was able to buy himself new eyeglasses and take his first vacation in 10 years. He told us, "I hope others can benefit from your efforts, as I did."

As the above examples underscore, the ability to use SSNs for matching purposes as a search term in commercial databases is critical to our efforts to give retired workers the benefits that they have earned. Without the ability to search using an SSN, a slight misspelling in a name, the presence or absence of a middle initial, and a less distinctive name can drastically reduce a pension plan's ability to locate pension fund beneficiaries. In our experience, searching with a retiree's SSN gives us an 85–90% chance of locating that retiree, compared to a less than 8% rate with only the ability to use a participant's name and address information.

If Congress were to enact legislation requiring prior consent on an individualized basis to use SSNs, this would effectively eliminate the availability of SSNs in the databases that we depend upon. Loss of this search term would dramatically increase the costs of locating former employees—costs that many fund administrators could refuse to pay. Moreover, in many cases, we would be unable to find the employee, and he or she would simply lose their pension benefits. Millions of dollars in vested accounts would be left behind.

Thank you, Mr. Chairman and Members of the Subcommittee, for the opportunity to express the views of the Pension Benefit Information. We know that Congress and this Subcommittee will continue to monitor this issue closely and we look forward to working with you to ensure that the positive uses of SSNs, that I have mentioned, continue to be protected.

Mr. COLLINS. Thank you. Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP

Mr. MIERZWINSKI. Thank you, Congressman. My name is Ed Mierzwinski with the State Public Interest Research Groups (PIRGs) national office and we are pleased to join the Committee today to testify once again on the importance of enacting legislation to protect Social Security numbers from misuse.

U.S. PIRG and the State PIRGs believe that the widespread availability of the Social Security number contributes to identity theft, which is well documented as one of the nation's fastest growing white collar crimes. The 1999 and 2000 amendments to the Drivers Privacy Protection Act championed by Senator Shelby form an excellent basis for changing the previously misguided congressional strategy of carving out exceptions to Social Security number protection and instead working to close loopholes. We look forward to working with the Committee on developing additional protections.

We believe the two most important things that the Congress could do would be to extend a strong anti-coercion provision on private sector use of the Social Security number and to close the recently narrowed credit header loophole which allows secondary use of the Social Security number without consumer consent. The credit header loophole has helped lead to the proliferation of information broker websites that make it easy for identity thieves and stalkers to obtain Social Security numbers and the other bits and pieces of the consumer's identity used to build a fraudulent identity in the consumer's name.

Any legislation that you enact should be simple, should be based on fair information practices, and contain as few loopholes and exceptions as possible. It is also critical that any new legislation not preempt or roll back or weaken any of the existing privacy protections, including those recently upheld by the courts in the Gramm-Leach-Bliley law and of course including the new Shelby amendments.

U.S. PIRG concurs with the views of our colleagues today from the Electronic Privacy Information Center and Privacy Times. We believe that your legislation should be simple. Probably you should extend Section 7 of the Privacy Act to private uses of the SSN, extend it to the commercial sector. The anti-coercion provision in H.R. 4857 I think is a good step toward doing that.

The other important provision in last year's bill, H.R. 4857, was its provision taking the Social Security number out of credit headers and moving them into the body of credit reports. Those are two very important provisions.

I think the other thing that you need to do is to look at what the commercial sector has done over the years in using the Social Security number. They have used it as a crutch. It is really not as accurate as they say and, in fact, based on our statistics from reports published by the Public Interest Research Groups, reports by the Privacy Rights Clearinghouse and even reports by the Federal Trade Commission as mandated by the Identity Theft Act of 1998, and their data are all up on their website, identity theft is skyrocketing. It is a major problem.

I talk to consumers. I talk to victims. I got a phone call today from a victim. I talk to them all the time. I also know how easy it is to do exactly what the investigators did this morning with their computer demonstration. It is easy to use Social Security numbers and other information to commit identity theft and I submit to you that protecting the Social Security number with some technology-forcing provisions that forces the industry to switch to a more precise and accurate number and stop using the Social Security number will actually reduce identity theft.

Last year, as you may know, consumer and privacy groups ended up opposing the bill that came closest to passing, the Amy Boyer law. We believe that the Amy Boyer law, although named for the first known victim of an Internet stalker, contained too many loopholes that would have allowed information brokers, private detectives and others to slip through its nominal protections. And, of course, loopholes is not what we want in any final legislation. We did think that H.R. 4857 was a better basis for legislation and we hope the Committee will work to enact a bill somewhat similar to that.

In terms of fair information practices, my testimony goes into great detail on the report that was issued in 1973 that talks about the fair information practices and the need to protect the Social Security number, which may provide the Committee with guidance.

Throughout the lobbying on privacy and Social Security numbers and other privacy issues over the last several years in the Congress, and I want to commend the numerous Republican members at the rank and file level who have been leaders on privacy, by the way, although I share the concerns of Mr. Hendricks that the very top levels of the leadership have had a disappointing record on privacy—throughout this debate on not only Social Security numbers but on other issues, industry groups have sought to dumb down the fair information practices, which are actually quite detailed. They believe that notice is enough.

Notice is not enough. Nor is notice and choice when choice is limited to only an opt-out some of the time. Consumers need to control the use of their personal information on an expressed opt-in consent basis all the time, not an opt-out some of the time.

My testimony goes into detail on the credit header loophole and the two recent court cases upholding the right of the government to protect privacy. My testimony also discusses why the voluntary regulations of IRSG just plain and simple are not good enough. And my testimony also details the problem of identity theft. I would be happy to answer any of the Committee's questions. Thank you very much.

[The prepared statement of Mr. Mierzwinski follows:]

Statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group

Chairman Shaw and members of the committee: We are pleased to present the views of the U.S. Public Interest Research Group on the misuses of Social Security numbers. As you know, U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups, which are non-profit and non-partisan consumer and environmental advocacy groups active around the country.

Summary

U.S. PIRG believes that the widespread availability of the social security number contributes to identity theft, which is well-documented as one of the nation's fastest growing white-collar crimes. The 1999 and 2000 amendments to the Drivers Privacy Protection Act by Senator Shelby form an excellent basis toward changing the previous misguided Congressional strategy of carving out exceptions to Social Security Number protections and instead working to close loopholes.[1] We look forward to working with the committee on developing additional protections.

We believe that the two most important actions Congress could take would be to extend a strong anti-coercion provision to private sector use of the Social Security Number and to close the recently-narrowed credit header loophole, which allows secondary use of Social Security Numbers without consent. The credit header loophole has led to the proliferation of information broker websites that make it easy for identity thieves and stalkers to obtain Social Security Numbers and other bits and pieces of a consumer's identity that are used to build a fraudulent identity in the victim's name. Any legislation enacted should be simple, based on Fair Information Practices, and contain as few loopholes and exceptions as possible. It is critical that new legislation not preempt or roll back existing privacy protection under either the Gramm-Leach-Bliley regulations or the Shelby amendments.

(1) Principles of Social Security Number Protection: Simplicity, With Few, If Any Exceptions and Loopholes

U.S. PIRG concurs with the views of our colleagues today from the Electronic Privacy Information Center (EPIC) and the Privacy Times. We believe that the most effective way to protect Social Security Numbers would be to enact simple, straightforward legislation that reins in the widespread non-statutory uses of the Social Security Number as an identifier in the private sector.[2] One simple way to do this would be to extend Section 7 of the Privacy Act,[3] which protects the Social Security Number in government uses with an anti-coercion provision, to the private sector. Your bill in the 106th Congress, HR 4857, included such a provision. It would have made coerced demand of a consumer's Social Security Number an unfair trade practice under Section 5 of the Federal Trade Commission Act.

Privacy expert Robert Ellis Smith,[4] the publisher of Privacy Journal and author of "Social Security Numbers: Uses and Abuses" (May 2001) has recently proposed a similarly simple Social Security Number protection scheme. Here is Smith's proposal, with his explanations in brackets:

> 1. "It shall be illegal to buy or sell the Social Security number of a person." [This is the source of much identity theft; it is always a secondary use of the SSN; and it is inconsistent with using the SSN as an AUTHENTICATOR of personal identity.]
>
> 2. "No person shall be required to provide a Social Security number on an application for credit or on a request for a copy of one's own credit report under the Fair Credit Reporting Act." [The FCRA merely requires satisfactory proof of identity to see one's own credit file. Use of SSNs to make a match between a requested credit report (by a credit grantor) and a credit report in a credit bureau's system has been the cause of confusion for credit grantors, nightmares for consumers, and identity theft. If credit bureaus did not rely on SSNs to make a match, 80 percent of identity theft would cease. There is a long list of case law to support the need for this provision.]
>
> 3. "No person shall be compelled or coerced into providing a Social Security number for any transaction unless there are income-tax consequences in the transaction or there is relevance to Social Security, Medicare, or Medicaid benefits. No person shall be compelled or coerced into providing a Social Security

---

[1] Senator Shelby's 2000 amendments to the Driver's Privacy Protection Act were incorporated as Section 309 of the Transportation Appropriations bill (PL 106–346) signed by the President 23 October 2000. The amendment requires states to obtain express consent of drivers before the sharing or selling of a driver's "highly sensitive personal information," including Social Security Number, photograph, image, or medical or disability information. In 1999, Shelby had incorporated these provisions into law as part of the Appropriations bill, but only for one year, while the 2000 amendment amends the DPPA itself. In 2000, the Supreme Court upheld the constitutionality of the DPPA in Reno vs. Condon.

[2] Ideally, such a bill would also narrow many of the government use exceptions that have been established over the years allowing the Social Security Number to be used as an identifier and matching element for secondary purposes unrelated to Social Security.

[3] Privacy Act of 1974, Public Law 93–579.

[4] See the Privacy Journal website for more information. Smith's latest book is "Ben Franklin's Web Site: Privacy And Curiosity From Plymouth Rock To The Internet" <http://www.townonline.com/specials/privacy/>

number on an application of employment until there has been a firm offer of employment. Any application for employment shall state that the request for the Social Security number prior to a firm offer of employment is voluntary." [This would essentially freeze demands for Social Security numbers in a way least disruptive to organizations currently relying on SSNs. It would tie demands for Social Security numbers to the two original purposes (SSA administration and federal taxes)—two uses that are at least anchored in long-standing law. Placing SSNs on job-application forms increases the risk of exposing them to fraudulent users of SSNs.]

4. "No institution of higher education or elementary or secondary school shall use a student's Social Security number as a student identification number." [An alarmingly high number of identity theft frauds originated from SSNs taken from universities. Deterring school systems from using the SSNs as a student ID number will permit parents to delay labeling their children with numerical IDs.]

Alternatively, several more comprehensive proposals were presented in the 106th Congress to protect Social Security Numbers. Most notably, HR 4857 (Shaw-Matsui-Kleczka) was favorably reported by the Ways and Means Committee.[5] The bill included two critical provisions. In addition to its strong private sector anti-coercion provision, HR 4857 incorporated provisions championed by Rep. Kleczka closing the so-called credit header loophole. Under an egregious 1994 decision of the Federal Trade Commission, credit reporting agencies (credit bureaus) have developed a thriving business selling Social Security Numbers without consumer consent. While a recent federal court decision upholding the Gramm-Leach-Bliley Act privacy regulations has narrowed the credit header loophole,[6] more needs to be done (see below).

In the 107th Congress, meritorious proposals include HR 1478 (Kleczka), HR 220 (Paul) and S 324 (Shelby) to protect Social Security Numbers. Among other Social Security Number bills with positive features in the 106th Congress was a proposal by Rep. Markey (HR 4611).

Unfortunately, the most prominent 2000 Senate proposal to ostensibly protect Social Security Numbers actually would have expanded commercial availability of Social Security Numbers. Originally intended to serve as a legacy for Amy Boyer, the first known victim of an Internet stalker, the Amy Boyer Law, as very nearly enacted into law,[7] was actually a Trojan Horse[8] and would have expanded commercial loopholes for obtaining Social Security Numbers, failed to protect Social Security Numbers on public documents and also would have preempted stronger state privacy laws.

We are, however, pleased that the Amy Boyer Law's chief sponsor, Senator Gregg, is working on a stronger bill this year. However, we believe that your stricter HR 4857 anti-coercion provision is a better approach than the weaker anti-coercion language in the 2001 proposal by Sens. Feinstein and Gregg, S. 848, which includes broad "credit check" exceptions that swallow its nominal anti-coercion rule. Any time the Congress determines that an exception is needed, it should more narrowly define the exception—in this case, for example, reference should be made to obtaining a credit report under the Fair Credit Reporting Act.[9] In addition, although its

---

[5] The Social Security Number Privacy And Identity Theft Protection Act of 2000, House Report 106-996, 24 October 2000.

[6] Individual Reference Services Group, Inc., and Trans Union LLC v. FTC (District of the District of Columbia) Civil Action 00-1828, 30 April 01, granting summary judgment to the Federal Trade Commission on all counts and dismissing plaintiffs' complaints with prejudice.

[7] The Amy Boyer Law, introduced as S. 2554, (Gregg), was incorporated as Section 626 into the Commerce-Justice-State Appropriations (HR 4690 RS) and passed into law as Section 635 of HR 5548, which was included in HR 4492 as sent to the President, but then was rescinded on the same day by language reversing its effect included in the Conference Report on HR 4577, the Consolidated Appropriations Act, (Labor-HHS Approps). Section 213 of HR 4577 amends HR 5548 by deleting a number of sections of HR 5548. Section 213(a)(6) of HR 4577 strikes the Amy Boyer Law (Section 635 of HR 5548). See page H12261 of the Congressional Record for 15 Dec 00.

[8] See the U.S. PIRG Fact Sheet, "Why The Amy Boyer Law Is A Trojan Horse" at <http://www.pirg.org/consumer/trojanhorseboyer.pdf>

[9] As another example, the law enforcement exception in S 848 makes collection of delinquent child support a "law enforcement" purpose. Does that extend the exception to allow any private firm collecting child support to take advantage of the exception? It appears to do so, despite well-documented circumstances where some private child support collection firms have abused debt collection laws. Last year, a controversial proposal originally included as Title III in HR 4469 (Nancy Johnson) before the Ways and Means Committee would have extended child support enforcement to private firms but did not become law. See "Problems At Child Support, Inc.,

Continued

business-to-business exceptions are more narrowly construed than the Amy Boyer Law's and also subject to a rulemaking, S. 848 still retains the weak, pro-information broker structure of the Amy Boyer Law's "professional and commercial" user business exceptions, rather than closing the credit header loophole.

We hope we can work with you, your staff, and the committee to ensure that any final legislation includes the strongest protections and the fewest exceptions possible to the use of Social Security Numbers for any purposes not associated with the Social Security Act. If the committee believes it is necessary to extend any exceptions at all allowing continued non-statutory collection of Social Security Numbers by the private sector, which has unfortunately come to depend on the Social Security Number as a crutch, then the committee should include technology-forcing time limits on private uses so that firms are forced to develop more accurate alternatives that do not pose the secondary use problems of continued use of the Social Security Number, which was originally intended only for Social Security and certain tax purposes.

(2) What Are Fair Information Practices?

A government report, produced by the Advisory Committee on Automated Personal Data Systems created by the U.S. Department of Health, Education, and Welfare in 1973, considered government use of social security numbers and issued the following recommendations: [10]

First, uses of the SSN should be limited to those necessary for carrying out requirements imposed by the Federal government.

Second, Federal agencies and departments should not require or promote use of the SSN except to the extent that they have a specific legislative mandate from the Congress to do so.

Third, the Congress should be sparing in mandating use of the SSN, and should do so only after full and careful consideration preceded by well advertised hearings that elicit substantial public participation. Such consideration should weigh carefully the pros and cons of any proposed use, and should pay particular attention to whether effective safeguards have been applied to the automated personal data systems that would be affected by the proposed use of the SSN.

Fourth, when the SSN is used in instances that do not conform to the three foregoing principles, no individual should be coerced into providing his SSN, nor should his SSN be used without his consent.

Fifth, an individual should be fully and fairly informed and of his rights and responsibilities relative to uses of the SSN, including the right to disclose his SSN whenever he deems it in his interest to do so.

More broadly, that report developed the concept of Fair Information Practices, which apply to any use of personal information on consumers or citizens. Collecting information for one purpose (Social Security) and using it for another (government sector matching, private sector locator services, etc.) without the individual data subject's consent violates those Fair Information Practices. The Fair Information Practices were incorporated in the Privacy Act of 1974 (for government uses) and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines. Information use should be subject to Fair Information Practices that limit information collection, guarantee its integrity, security and accuracy and provide for the following consumer rights: notice, consent, access, correction, liability for violations.[11]

Fair Information Practices are discussed in numerous contexts in the Congress today. Unfortunately, many industry-supported bills and nearly all industry "studies" seek to dumb-down the comprehensive Fair Information Practices to unacceptable levels.

- First, industry groups seek to substitute a weaker opt-out choice, instead of providing express opt-in consent before secondary uses,
- Second, industry groups claim that notice is enough. They claim that disclosure and correction are unnecessary.
- Third, they contend that either agency enforcement or self-regulation is an adequate substitute for a consumer private right of action.

Business, Complaints Increase For Specialized Collection Firms" 18 May 2000, Washington Post, Caroline E. Mayer and Jacqueline Salmon.

[10] Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, (1973) 124. (emphasis theirs)

[11] Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html>

Notice is not enough. Nor is "notice and choice," especially when choice means the virtually meaningless right to opt-out, rather than the right to expressly consent, or opt-in. Consumers and citizens are both entitled to and need the full panoply of rights and protections proposed by the 1973 committee, especially as recordkeepers develop new, unanticipated secondary uses, and newer, more powerful mechanisms for collecting, slicing and dicing data.

(3) What Is The Credit Header Loophole That Allows Easy Availability Of Social Security Numbers?

In 1994, the Federal Trade Commission granted an exemption to the definition of credit report when it modified a consent decree with TRW (now Experian). The FTC said that certain information would not be regulated under the Fair Credit Reporting Act. The so-called credit header loophole allowed credit bureaus to separate a consumer's so-called header or identifying information from the balance of an otherwise strictly regulated credit report and sell it to anyone for any purpose.

Credit headers include information ostensibly not bearing on creditworthiness and therefore not part of the information collected or sold as a consumer credit report. The sale of credit headers involves stripping a consumer's name, address, Social Security Number and date of birth from the remainder of his credit report and selling it outside of the FCRA's consumer protections. Although the information, marketing and locater industries contend that header information is derived from numerous other sources, in reality, the best source of credit header data is likely financial institution information, which is updated regularly.

Two recent court decisions have narrowed, but not closed, the credit header loophole. In March 2000, the FTC had banned target marketing from credit reports and also held that dates of birth are credit-related information and removed them from headers. That decision was upheld on 13 April 01 by the U.S. Court of Appeals for the DC Circuit in a strong victory for privacy protection, since it also upheld the constitutionality of the Fair Credit Reporting Act.[12]

The final Gramm-Leach-Bliley financial privacy rules issued later that spring by the FTC and 5 other federal financial agencies defined Social Security Numbers as non-public personal information. That decision was upheld on summary judgment on 30 April 01 by U.S. District Court Judge Ellen Huvelle.

The result of the district court's strong ruling, if upheld, is that credit bureaus cannot share credit header information (including Social Security Numbers) obtained from financial institutions, since the financial institutions have failed to provide consumers with notice of this information sharing practice and the right to opt-out of nonaffiliated third party sharing, as required by the Gramm-Leach-Bliley regulations. However, once banks and other financial institutions modify their defective privacy notices to describe this sharing, the protection will then only apply to consumers who exercise their right to opt-out.

While this is a very strong, pro-privacy decision, we believe that it still makes sense for the Congress to enact legislation closing the credit header loophole by statute. Even if Gramm-Leach-Bliley continues to be upheld, ultimately, consumers would have to exercise their modest opt-out rights to gain protections they should have by law. For example, HR 1478 (Kleczka) would re-define all sensitive information, including Social Security Numbers, held in credit report files to be protected by the Fair Credit Reporting Act as part of credit reports "except the name, address, and telephone number of the consumer if listed in a residential telephone directory available in the locality of the consumer."

(4) Why Isn't Voluntary Self-Regulation Good Enough?

In 1997, the credit bureaus and several of the firms that traffic in the credit headers that the credit bureaus sell formed a so-called "self-regulatory" association known as the Individual References Services Group. The organization says its "principles impose significant restrictions on the access and distribution of non-public information, such as non-financial identifying information in a credit report. For ex-

[12] At the time, Equifax voluntarily agreed to stop target marketing from credit reports. Trans Union, on the other hand, refused, and then led the FTC through eight years of litigation, while it continued to use credit reports to generate target marketing lists in defiance of the FTC. On 1 March 2000, the FTC again ordered Trans Union to stop, although it agreed to stay the ruling while Trans Union appealed yet again. <http://www.ftc.gov/opa/2000/03/transunion.htm> Last month, in rejecting Trans Union's constitutional arguments in that appeal, the U.S. Court of Appeals said "Contrary to the company's assertions, we have no doubt that this interest—protecting the privacy of consumer credit information—is substantial." United States Court of Appeals For The District Of Columbia Circuit, 13 April 2001, No. 00–114, Trans Union Corporation v. Federal Trade Commission, On Petition for Review of an Order of the Federal Trade Commission.

ample, Social Security numbers obtained from non-public sources may not be displayed to the general public on the Internet by IRSG companies."[13] (How does IRSG protect Social Security Numbers obtained from other than "non-public sources?")

Despite these nominal voluntary rules, U.S. PIRG, the Privacy Rights Clearinghouse, other advocates, reporters, and identity thieves and stalkers have found that SSNs can still be purchased from websites. We strongly support closing the credit header loophole because, even if the IRSG's voluntary rules were effective in halting the sale of SSNs to the general public, it is easy to use a "pretext" to obtain SSNs from one of the many sites on the Internet that purports to only sell it to qualified requestors.

We also support Congressional review of the adequacy of the IRSG's self-regulatory system. While the FTC encouraged the formation of the IRSG in 1997, it said at the time that the IRSG Principles did not meet all Fair Information Practices. The FTC also said that the IRSG must make public a "Summary" of the results of "third-party assessments," or audits, of its members. To our knowledge, while the IRSG provided the FTC in 1999 with what we believe to be a highly unsatisfactory letter[14] stating that the assessments were completed, no summaries have ever been made public.

Unfortunately, the 106th Congress Amy Boyer Law and several 107th Congress proposals include private sector business-to-business loopholes allowing "professional and commercial" users continued access to Social Security Numbers. The Amy Boyer Law would have even expanded the access now allowed, under IRSG's own weak voluntary operating rules.

To stave off legislation four years ago, IRSG proposed to FTC a set of principles its members are required to operate by. Under one principle, so-called "professional and commercial users" can use Social Security numbers, but only if displayed in truncated form. Here is the provision:[15]

> B. Commercial and Professional Distribution of Non-Public Information: Individual reference services, when they limit the non-public information content of their products or services as set forth below, may distribute such products or services only to established professional and commercial users who use the information in the normal course and scope of their business or profession and the use is appropriate for such activities.
>
> 1. non-public information products or services distributed pursuant to this subsection shall not include:
>
> a. Information that reflects credit history, financial history, medical records, mother's maiden name identified as such, or similar information;
>
> b. Certain information like social security number and birth information unless truncated in an appropriate and industry consistent manner.

Yet, the Amy Boyer Law included specific language exempting "professional and commercial users," exactly the phrase from IRSG. These firms—including private detectives, Internet information brokers, debt collectors and skip tracers, would appear to gain a new right to use full **untruncated** Social Security Numbers under law, even though their own trade association had previously apparently limited them to truncated uses, to protect consumer privacy. In some states private detectives are not regulated at all, in most other states, private detectives are under-regulated at best.

(5) What Does It Mean To Be An Identity Theft Victim?

In our view, the mere fact that Social Security Numbers were never intended as a national identifier yet are being routinely used in the private sector for secondary purposes without consent is adequate reason for the committee to act. Yet, the Social Security Number is also the key to a consumer's financial identity. Easy access to Social Security Numbers aids identity thieves and stalkers.

Just as one of the other witnesses has demonstrated today, I, along with other consumer and privacy advocates, have often used pretexts to demonstrate how easy it is to obtain Social Security Numbers from on-line information broker websites, despite supposed limitations on disclosure to unauthorized persons claimed by the sites. While identity thieves can also obtain social security numbers from other sources, such as drivers' licenses in some states, student IDs, and medical records, why go to the trouble when you can log onto the Internet?

The committee has heard today from several identity theft victims. The committee has also heard from experts about how easy it is to buy Social Security Numbers.

---

[13] See http://www.irsg.org

[14] See Letter from IRSG's Ron Plesser to FTC, 28 April 1999, <http://www.irsg.org/html/letter_to_the_ftc.htm>

[15] < http://www.irsg.org/html/industry_principles_principles.htm>

This winter, stories about identity theft victim Tiger Woods were prevalent. In March, newspaper stories reported on how sloppy financial industry security practices enabled a high-school dropout working as a busboy to steal the identities of numerous celebrities:

> Using computers in a local library, a Brooklyn busboy pulled off the largest identity-theft in Internet history, victimizing more than 200 of the "Richest People in America" listed in Forbes magazine, authorities say. Abraham Abdallah, 32, a pudgy, convicted swindler and high-school dropout, is suspected of stealing millions of dollars as he cunningly used the Web to invade the personal financial lives of celebrities, billionaires and corporate executives, law enforcement sources told The Post.[16]

In May 2000, California PIRG and the Privacy Rights Clearinghouse released a report[17] summarizing the results of a survey of victims. We found that identity theft victims had labored 2–4 years or more to rid themselves of an average of $18,000 in fraudulent accounts. However, worse than cleaning up the financial mess is the enormous time commitment victims spend cleaning up their lives:

Respondents spent an average of 175 hours actively trying to resolve problems caused by the theft of their identity. The victims reported missing several days or weeks of work to put their lives back together, and two people even reported losing their jobs due to the time devoted to identity theft resolution. A victim from California felt that resolving her problem was "nearly a full-time job." Robin, a victim from Los Angeles, explains, "One bill—just ONE BILL—can take 6-8 hours to clear up after calling the 800 numbers, waiting on hold, and dealing with ignorant customer representatives." She concludes, "The current system is not created for actual assistance, it is created to perpetuate the illusion of assistance."[18]

> Recently, the Federal Trade Commission published a detailed report summarizing identity theft complaints to the agency since passage of 1998 legislation requiring it to establish a database and clearinghouse. Highlights of the report,[19] which covers the period from November 1999 through March 2001, are the following:
>
> • The volume of calls to our Hotline has grown dramatically. In November 1999, the Hotline answered about 445 calls per week. By March 2001, the Hotline was answering over 2,000 calls per week.
>
> • Taken together, the information in the Clearinghouse Database shows that identity theft has a devastating effect on consumers' lives. Most consumers have no idea how this happened to them and do not discover their personal information has been misused for more than a year, and sometimes as long as five years.
>
> • Victims must spend significant amounts of time contacting creditors and credit reporting agencies in order to repair the damage done to their credit histories. In the meantime, they are often unable to obtain credit and financial services, telecommunication and utility services, and sometimes employment. Wages may be garnished, or tax refunds withheld, due to the bad debts or other penalties levied in their names.
>
> • Where the identity thief has created a criminal record in the victim's name, consumers report having driving and other licenses revoked, failing background checks for employment and other purposes, and even being arrested and detained.

The difficulties victims experience as a result of identity theft are of great concern to the FTC.

(6) Who Else Wants Your Social Security Number? Stalkers.

As the Christian Science Monitor and Nando News explained last year:

---

[16] See New York Post, 20 March 2001, "HOW NYPD CRACKED THE ULTIMATE CYBERFRAUD" <http://dailynews.yahoo.com/htx/nypost/20010319/lo/how_nypd_cracked_the_ultimate_cyberfraud_1.html>

[17] "Nowhere To Turn," Benner, Givens and Mierzwinski, CALPIRG and Privacy Rights Clearinghouse, 1 May 2000. See <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>. We have released two previous reports on identity theft "Theft of Identity: The Consumer X-Files", CALPIRG and US PIRG, 1996 and "Theft of Identity II: Return to the Consumer X-Files", CALPIRG and US PIRG, 1997, as well as four reports on errors by credit reporting agencies since 1991, most recently "Mistakes Do Happen," 1998.

[18] See "Nowhere To Turn," <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>

[19] See Figures and Trends On Identity Theft November 1999 through March 2001 Federal Trade Commission <http://www.consumer.gov/idtheft/reports/rep-mar01.pdf> Also see accompanying charts. According to the FTC identity theft complaint summary, "The FTC's Identity Theft program, established pursuant to the Identity Theft and Assumption Deterrence Act, Pub. L. No. 105–318, 112 Stat. 3007 (1998)(codified at 18 U.S.C. § 1028)(the "ID Theft Act"), assists consumers who are, or are concerned about becoming, identity theft victims."

> So you think your private information is relatively safe? Think again. For a mere $49, someone can hop on the Internet, give a company your name, wait a few days, and bingo: up pops your Social Security number. Want someone's bank account balance? That costs $45. An unpublished telephone number? $59.[20]

The reporter in that story wasn't writing about the "white-collar" crime of identity theft, however. Actually, the story was about the brutal stalker murder of Amy Boyer in New Hampshire. As the story explains:

> Her killer, a man obsessed with her since 10th grade, left evidence that he tracked her down through the online personal-data service Docusearch.com.
>
> On his own Web site, Liam Youens detailed his plans for killing Boyer, including how he found her: "I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment. It's accually obscene what you can find out about a person on the internet." After shooting Boyer, Youens turned the gun on himself.
>
> Stunned that such information could be purchased by anyone, Boyer's parents, Tim and Helen Remsburg, recently filed a suit against Docusearch.com. They also testified before a Senate subcommittee about the killing.[21]

(7) What Other Actions Would Protect Social Security Numbers From Misuse?

Using the Social Security Number as a employment ID, medical ID, college student ID or motor vehicle ID leads to identity theft or other problems. As noted above, last year Congress made permanent the 1999 Shelby amendment expanding consumer privacy rights in information held by state motor vehicle departments. The committee has heard testimony today about the widespread use of Social Security Numbers as student identification and as a health record identifier. These uses should be phased out, by enactment of trigger-based, sunset regulation prohibiting the use of Social Security Numbers in the private sector after a certain time.

Conclusion

While the U.S. has a strong history of privacy protection, our statutory privacy protections are a patchwork—what industry prefers to call a "sector-by-sector" approach. Yet, whatever the merits, if there ever were any, of the industry-prescribed sector-by-sector approach, it is rapidly obsolescing as industry sectors converge. The names of the videos you rent are better protected than your not-so-confidential bank account balances, credit card records and medical history. U.S. PIRG strongly supports enactment of over-arching privacy legislation that requires all businesses to protect consumer and customer information under laws based on Fair Information Practices and gives consumers enforceable rights if their personal information is misused.

The basic structure of information privacy law is to place responsibilities on organizations that collect personal data and to give rights to individuals that give up their data. This is sensible for many reasons, including the fact that it is the entity in possession of the data that controls its subsequent use. Information privacy law also promotes transparency by making data practices more open to scrutiny and encourages the development of innovative technical approaches.[22]

We want to thank you, Mr. Chairman, for the opportunity to present our views on the need for strong privacy protections to protect Social Security Numbers from misuse. We look forward to working with you on this and other matters to guarantee the privacy of American citizens. Restricting the widespread availability of Social Security Numbers is one of the most important solutions to the identity theft epidemic.

Mr. COLLINS. Thank you. Thank you all for your testimony. Mr. Becerra, any questions?

Mr. BECERRA. Mr. Chairman, thank you. Let me see if I can limit the number of questions I have here.

---

[20] "Suit alleges online privacy breach had deadly consequences" By KRIS AXTMAN, The Christian Science Monitor (May 9, 2000 1:34 a.m. EDT http://www.nandotimes.com)

[21] Ibid.

[22] See the "Privacy Law Sourcebook, 2000: United States Law, International Law and Recent Developments," by Marc Rotenberg, Electronic Privacy Information Center, for a comparision of all important privacy laws.

Let me ask Mr. Dugan and perhaps Mr. Plesser and Ms. LeRoy first if they can comment on based on the legislation from last year, what you would not want to see in the bill. What do you object to?

Mr. DUGAN. Mr. Becerra, we had several concerns that, for example, prohibitions on sales of information could sweep in things that are routinely done in business-to-business transactions that really do not raise of the kinds of concerns that we talked about this morning.

For example, it is critical for two financial institutions that are trying to transfer assets to each other to be able to use Social Security numbers. SSN's are often the only way that you can make sure that the right money is going from one financial institution to a totally unrelated financial institution, and I do not think there is anybody who thinks that is an illegitimate type of transaction. So when you talk about "sale," you have to be quite careful about what exactly it covers so that it does not unintentionally sweep in that kind of unintended use.

We are also concerned that the effort to restrict SSN use more generally would prohibit financial institutions from using it for the kinds of fraud detection purposes that they use it for now.

One point I think is worth making is to respond to the implicit suggestion that financial institutions somehow benefit from, or favor, identity theft. In fact, just the opposite is true. Financial Institutions absolutely oppose identity theft not only for the pain it causes customers, but also because it is expensive. We, too, are very much in favor of measures that are very targeted to that identity theft and to prevent it. It is just that we also believe that there are real beneficial uses of Social Security numbers to detect identity theft and other benefits, as well.

Mr. BECERRA. Let me just make sure you are focusing on that because I do not want to run out of time and I do have several questions I want to ask.

Mr. Plesser and Ms. LeRoy, if you could add to that. And I know what some of the governmental concerns are and I think those are legitimate but in terms of the private sector, I am trying to figure out what it is that the private sector would object to with regard to last year's legislation.

Mr. PLESSER. Let me just echo those comments. I think the biggest concern we have now is the exemptions do not cover many of the positive purposes and uses that I think we have been discussing this morning. They would not allow what Mrs. LeRoy does. They do not allow finding a lawyer who identifies witnesses and takes their Social Security number because five years later they are going to need them to testify and people move. Twenty percent of America moves every year.

So, the question is we want to be able to find lost witnesses. We want to be able to provide information so that heirs can be located on wills. Perhaps a will was done 30 years before. I think there are a lot of positive uses in business, the business-to-business use.

We would support the restriction of the Social Security number from being displayed to the public. I think last year use was not restricted and we think that was positive but the purchase and sale—in order to use it, it has to be obtained.

So those are really the points we have talked to staff about. We have had very positive dialogue with staff and we continue to feel that that will be fruitful and we would like to work with the Committee on that.

Mr. BECERRA. Ms. LeRoy?

Ms. LEROY. May I say that every day we deal with people who we find and communicate to them that they have money coming to them from really a forgotten source. And while the flavor I hear is that the American public is outraged that people do have access to their Social Security numbers, this is not an issue we encounter. Out of 200,000 people per year perhaps five have an objection: Who gave you my Social Security number? How did you get it? And when we explain fully——

Mr. BECERRA. Let me have you focus because I am going to run out of time and I am just trying to find out what you object to in the legislation as it was proposed, if you are familiar with it, or the uses that were being prohibited through last year's legislation. I am trying to get a sense of what you do not want to see in it or maybe you want to tell me what you can see in it.

Ms. LEROY. What I would like to see is legitimate business practices.

Mr. BECERRA. Be exempted?

Ms. LEROY. Yes.

Mr. BECERRA. Which are those legitimate business practices that you would like to see exempted?

Ms. LEROY. I think when someone has an asset for a person, that the person having their Social Security number be utilized to find them, they are better off than they were before.

Mr. BECERRA. So assets. What else?

Ms. LEROY. Probably the greater good. I know the blood banks like to use that to find tissue donors and blood donors in emergencies.

Mr. BECERRA. Really what you are talking about is the need for some unique identifier for individuals to ensure that when you give this information or this financial asset or this greater good, this benefit to the individual, that you are giving it to the right person.

Ms. LEROY. Exactly.

Mr. BECERRA. And right now we use the Social Security number for that purpose of acting as the unique identifier but there is nothing that stops us from creating some other type of unique identifier, right? And the problem we have right now is the Social Security number was never created to be that unique identifier and it, of itself, is not the best or it can be a better and more integrated form of identification if the Social Security Administration had first and foremost meant it to be that. But it was never meant to be that, so it is an inefficient identification number to begin with. We have nothing else in place to use and it does cause problems and it puts it at the foot of the Federal Government to try to maintain that identifier.

Let me ask a question of you, Mr. Dugan, because you mentioned the transactions, verifying transactions and the sale of that information. One financial institution can provide the information to another financial institution so you can make sure the transfer of assets or the sale of assets or purchase can be done. Why does one

business have to charge the other for that? Why can you not just provide it free?

Mr. DUGAN. I'm sorry?

Mr. BECERRA. Merrill Lynch sells information to somebody else.

Mr. DUGAN. Actually, what I was trying to get at is suppose you want to transfer your assets from Merrill Lynch to Solomon Smith Barney.

Mr. BECERRA. Okay, does Merrill Lynch charge Solomon Smith Barney?

Mr. DUGAN. No, but they have to have a way to make sure that the John Dugan who walks in in one place is the John Dugan in the other and there may be hundreds of John Dugans. And unfortunately or fortunately, depending on how you look at it, the one really common unique identifier we use with systems that are not closed systems is the Social Security number.

The other point I would just make is that financial institutions have a set of restrictions already in place under Gramm-Leach-Bliley that apply to Social Security numbers, and when SSN's are sold there are restrictions on their redisclosure and reuse. So, an exemption for financial institutions is something that we would want to see in any legislation that is enacted.

Mr. BECERRA. But other than something already written in Federal law, why should we allow the sale or purchase of a Social Security number?

Mr. DUGAN. It depends on——

Mr. BECERRA. Why should somebody make money off of the sale of a Social Security number, which is a number generated by the Federal Government for purposes of Social Security benefits?

Mr. DUGAN. If, for example, a consumer did not object to the sale to a service that was allowing people to track down pension benefits, there may be perfectly legitimate reasons for doing that. That is number one.

Number two, if you define "sale" too broadly you are going to sweep in things that you do not want to sweep in.

Mr. BECERRA. Well, why would a consumer want to allow his or her Social Security number to be sold?

Mr. DUGAN. Well, what do you call it, for example, when your Social Security number is used in the process of creating a credit report where it is provided to a third party as part of a process to make sure that that person's credit is good? We have the most efficient credit system in the world and the reason why we do is because we have the most efficient sharing of information in the world.

Mr. BECERRA. So somebody is making money off of that identifier, being able to use that identifier.

Mr. DUGAN. And the consumer is benefiting because the cost of credit is much, much lower in this country than anyplace in the world.

Mr. BECERRA. So as we try to solve the issues of identity theft and the problems with correct identifiers and somebody fraudulently securing a Social Security number, the taxpayer pays for us to generate those numbers, correct the fraud, go after those who commit the fraud. A credit card company gets to charge anyone who wishes to get a credit report of an individual money for the

use of that report or to disclose that report. Somehow we have to clean up the Social Security number and its use for that identification purpose but unless we charge the taxpayer, you all will not have an identifying number to use.

Mr. DUGAN. And that is our concern. We are worried about throwing the baby out with the bathwater. There are many things like what we talked about this morning where people are selling fake Social Security IDs. And, by the way, I think there are laws on the books that can be enforced to go after that sort of thing, which are real abuses that have to be addressed.

It seems to me it is a very different thing if in the way you address that kind of identity theft you end up—not intending to—but you end up impairing things that produce real benefits to consumers. That is the problem.

Mr. BECERRA. And I would love Mr. Hendricks or Mr. Rotenberg or Mr. Mierzwinski to chime in but my difficulty is that we have to take care of this identity thing. We have to do something to address the fraud. We also want to make sure that whether it is public or private enterprise that there are opportunities to have some way to identify people as being who they claim to be.

There is nothing unique about the Social Security number other than it became a pretty universal number. So, I guess what we are trying to do is grapple with how we try to maintain the Social Security number for what it was intended to be used for and perhaps allow it to be used for things that were not at first contemplated.

And if Mr. Hendricks or Mr. Rotenberg have any comments or Mr. Mierzwinski, I would love to hear how you respond to those who are in the private sector or in government, as well, who say that we have no choice but to use these numbers in order to continue in business.

Mr. HENDRICKS. Social Security numbers are used in a wide variety of contexts and they are mandated by Congress to be used by banks.

Let me first say that I think legislation is necessary to stop the abuses that we have talked about, the kind of bill that came out of this Committee last year, because if you look at the websites selling the Social Security numbers, the IRSG companies very likely could be the sources of that information that these guys are selling. And the IRSG companies need to do an audit where they buy from these brokers and trace it back to find out the source of the information.

Mr. BECERRA. Stop right there.

So, Mr. Plesser, how do you respond to that?

Mr. PLESSER. First of all, I respond that they are not the source. The IRSG companies absolutely have not been the source of those records since 1977. When we make those searches on Dog pile and others we find it very difficult to find the information.

I had a reporter from the National Journal who told me that in making her search they had to go to 100 sites. They may be from old sites, from old information, but they are not coming from the credit-reporting agencies. We are pretty certain of that in terms of anything past 1997. It may be that prior to 1997 those databases are still around and people are using them. And I think a lot of those services probably are pretexting—there is a time delay in

many of them. We do not know that they are really getting them from open-ended databases. Many of those sites at the bottom of them say we are a private investigator and then they will go ahead and do a pretext interview or a pretext call and get the Social Security number.

So, I think that the problem is a legitimate one but I do not think the causes or the source of the information was from the IRSG companies.

Mr. HENDRICKS. I think that Chairman Shaw asked the right question. Where are all these numbers coming from? They make them available in 15 to 30 seconds. They have to be available in automated systems.

It is ironic that these companies that specialize in audit investigation are not doing the most fundamental audit investigation to ensure that their databases are not being used for these purposes.

I think ultimately you are going to have to look at the Fair Credit Reporting Act as a model of what to do. You have to have a purpose test. The goal is the information collected for one purpose not be used for other purposes without people's consent.

One of the reasons is that when information is used outside of its context the way the Social Security number has been, then data integrity suffers, too. So when it was created for wage reporting and now it is used in the financial services, then the unintended consequence is that fraudsters realize this can be used to create fraud.

So, I think we have to start with the idea of basically a moratorium so there will be no more authorized uses, we look at specifying what purposes will be allowed through good public debate. And then pretty soon technology—Mr. Rotenberg can tell you that technology has some solutions for this. There are ways now of anonymizing information so it can only be seen behind fire walls, too, and in the future that could hold out some promise not to put the genie back in the bottle, but at least spank the genie.

Mr. ROTENBERG. I would just say that I think the problem with the misuse of the SSN are likely to accelerate. One of the very interesting things about the reporting of identity theft of which we were aware when we did the Greidinger case 10 years ago was that the problem at that time was just emerging, there was not the easy on-line accessibility that you have today or the increasing use of the SSN across the private sector for a whole slew of unrelated purposes.

The SSN is literally the flypaper of the information age: You hold it out there and anything with the same number will start sticking to it. So we need to find a way, I think through legislation, to restrict its use as the de facto identifier.

It was never intended, as you said, for this purpose. The problem of having an exception that says legitimate business purpose, is that, any purpose presumably done in good faith could be a legitimate business purpose.

As to Mr. Dugan's concerns, I think one of the ways to resolve these is that where the transfer takes place with the SSN in the context of financial institutions that are required to link a tax identification number with an asset, no one would reasonably object that that tax identification number follows the asset as it moves

between institutions. But that is really not the type of problem that has been described today. I think it is important that we focus on the real problem, which is the open-ended unrestricted use of the SSN, the real source of the identity theft problem.

Mr. MIERZWINSKI. Just very briefly, Congressman, I want to make the point that the financial industry's practices are just inadequate and unbelievably, the number of mistakes that they make in credit reporting leads not only to identity theft but many consumers, many of your constituents paying too much money for credit because of mistakes in their credit report causing their credit scores, their risk scores, to be lower than they should be and probably costing consumers billions of dollars.

As I think Mr. Hendricks pointed out earlier and the officers discussed earlier, you do not need to be the Russian mafia to commit identity theft. You can be an unemployed high school drop-out working as a—well, actually not unemployed—you can be a high school drop-out working as a busboy and you can type in the Social Security number of VIPs and have their credit transferred into your name. That is how easy it is.

If I know your Social Security number and I submit a credit application in your name at a new address, these systems are so poorly designed that I am going to get the credit in your name and that is unacceptable.

So we need to do more than just protect the Social Security number. I think we need to impose some higher standards on the credit reporting and the financial industry. Thank you.

Mr. BACARISSE. Congressman, may I take a moment just to remind the Committee—of course, you are well aware that there is in the government side on the child support area there is a key need for that data element to exist in order for the government to go after the $50 billion in unpaid child support that is out there in this country.

So, on the one hand, we have a certain segment of the population that is very interested in seeing the government perform better there at all levels. Thank you.

Mr. BECERRA. I get confused trying to just think about this or ask the question. Certainly we have to resolve this, Mr. Chairman. I think we do need to move forward with something. Obviously there are some legitimate uses of the number and there are some needs for the private and public sectors to continue to engage in their business but this is just going to get worse, as somebody just said.

I do not know what we do. Unless there can be some reconciliation between those who believe that the bill that we had last year was too restrictive and those who believe it does not go far enough, we will not go anywhere. I would just hope that we can come up with something because we do see too many cases like the two individuals who were here recently, earlier testifying about the abuses that occur.

I will yield back.

Mr. COLLINS. Thank you, Congressman.

It is a typical political problem. We have friends for it and friends who are against it and we are for our friends. The problem

here is theft and the concern is punishing the good guys rather than those who commit the theft.

If not the Social Security number, what number? What would be used for an identifier? Anyone. What would be used? How would you identify people?

I see in part of the report here that prior to '76 there was a major credit card bureau that did not use this as an identifier. What did they use?

Mr. HENDRICKS. They just used names and addresses at that point and their databases were not as big. And what happened was that the Social Security number was just laying there. Mr. Rotenberg said it was like the flypaper. To me it was like a lamb chop and all these wolves are circling and it was just too convenient to use.

Right now even the credit reporting agencies can do searches based on name and address. They have different information fields that they can use. But now that they have incorporated the Social Security numbers into their system it is an integral part of their system. Congress has mandated its use by the banks. It is an integral part of the banking system and I do not see that changing any time soon.

But, I think we can stop newer uses from spreading. To answer your question, the technology allows information to be compiled, searched and merged without using a Social Security number. You have other fields, like name, address, zip code. So, the technology is getting better to be able to do it so that it does not need to rely on a Social Security number.

Mr. COLLINS. But I can find that in the local telephone directory, name and address.

Mr. HENDRICKS. Phone number?

Mr. COLLINS. Yes. Well, not the phone number. I can find a person's name. I mean I can go to the telephone directory and find the names. What is to keep me from using those names in a false way to commit a theft? What we are dealing with is a number.

Prior to '76 when they did not use the number, do we have any numbers, any data that indicates the number of fraud and abuse or theft that occurred in the financial world?

Mr. ROTENBERG. As I recall, Congressman, it was about 10 years ago that the Attorney General started reporting on the use of the SSN in credit card theft because it became increasingly a part of that type of commission of crime as it became more accessible, and this is in support of my point that I think the problem is likely to increase.

But, the other point I wanted to make is in response to your question about systems of identification. It is true, we have many systems of identification. You have an account number for your credit card, for your utility bill, for your telephone number. These account numbers are unique to the institutions, which create unique account numbers. They do not use the Social Security number because they are trying to establish some confidentiality in the relationship with you in the information that they have about you, the bills that they send to you. It is standard practice. And it is a good practice.

Mr. COLLINS. That is my point. How many cases of credit card abuse were there last year? Anyone know? How many credit cards were stolen and misused last year?

Mr. MIERZWINSKI. Two years ago I believe the General Accounting Office reported to this Committee that in its studies it found that one of the credit bureaus reported 500,000 calls a year pertaining to identity theft. I think about one third of those may have been people inquiring about finding out more information but I think most people think it is in the half-million range today.

The Federal Trade Commission's most recent statistics required by the new law say that their number of phone calls has increased from the end of 1999, 449 calls a week, to about 2,000 calls a week.

Mr. COLLINS. This is on credit card abuse?

Mr. MIERZWINSKI. This is on identity theft, Congressman.

Mr. COLLINS. I am talking about credit card——

Mr. MIERZWINSKI. You have to ask the industry for credit card data but our reports have found it very difficult to compile credit card data. The industry looks at a lot of it as proprietary and they calculate fraud differently, but I would ask the industry witnesses to provide you with that.

Mr. COLLINS. Does anyone have any idea how many credit card thefts there were last year?

Mr. HENDRICKS. On the one hand, the European Union said credit card fraud itself, not identity but credit card fraud itself was up 50 percent in the last year and they attribute some of that to growing on line and the fact that organized crime are getting into hacking and getting credit card numbers. Industry people have told me in the U.S.——

Mr. COLLINS. Fifty percent of what?

Mr. HENDRICKS. It was up 50 percent. I am sorry. I have to provide that for the record.

Mr. COLLINS. Mr. Dugan, do you have a number?

Mr. DUGAN. I was just going to say we will be happy to provide that for the record. I do not.

Mr. COLLINS. The point is that we had 95,000 reports of misuse of the Social Security number. How many reports of misuse of a credit card, stolen or whatever, occurred last year? It is a different number, different credit card numbers.

Mr. HENDRICKS. Yes. I am sorry; the credit card industry still says—the U.S. industry folks I spoke to said it is still a very small percentage, like 1 percent of their transactions or fewer is credit card fraud. But that is why one of the solutions that people are starting to look at is disposable credit card numbers so that the credit card numbers are only good for one transaction.

Mr. COLLINS. I had one of my credit cards stolen.

Well, we have 95,000 reports of misuse of the Social Security number and we have 200,000 reports of good use of the Social Security number. What do you think? Which outweighs what?

Mr. HENDRICKS. Well, the misuse of the Social Security number—you are citing the Social Security Administration's numbers. That is just calls to one hotline. The calls to the Federal Trade Commission, the misuse of Social Security numbers has to be running well toward a million right now if you include the police agencies in California, the Federal Trade Commission Clearinghouse,

the Privacy Rights Clearinghouse, all the different places that are taking complaints. The numbers are much higher than 95,000.

Mr. COLLINS. Well, why would the inspector general report to this Committee in 95,000?

Mr. HENDRICKS. That is the ones going directly to him.

Mr. COLLINS. Directly to Social Security?

Mr. HENDRICKS. Yes.

Mr. COLLINS. And that is where it should be reported.

Mr. PLESSER. The 200,000 is just the one company.

Mr. COLLINS. Sir?

Mr. PLESSER. And the 200,000 is just the one company.

Mr. COLLINS. How many companies are there? You say you represent what, 14?

Mr. PLESSER. Fourteen companies.

Mr. COLLINS. How many other companies are there?

Mr. PLESSER. Excuse me?

Mr. COLLINS. How many other companies beyond the 14?

Mr. PLESSER. It would be hard to count. There are probably a lot of companies, smaller companies beyond. I do not think there is any fairly substantial companies in the reference services area that has not a member of the group. There are probably a lot of these fly-by-night guys who are up on the Web with illegal activities that certainly are not members of the IRSG.

Mr. COLLINS. These people on the websites, we all agree that is quite a problem. Where do they get that data? What is the easiest access for them to obtain their data?

Mr. PLESSER. My own view on that is that many of it, and I would be happy to have a dialogue with the investigator from the Social Security Administration, I think many of that, I think the time delay was not 15 to 30 seconds. I think the time delay they talked about was 15 minutes or 30 minutes and in most of the cases, many of the cases I am aware of, it takes 24 hours to get the response and I think a lot of that is individual——

Mr. COLLINS. That is not my question, though. My question is not how long it takes them to download, to transmit to you the information, but where do they get their information? This gentleman on the end down here.

Mr. BACARISSE. Congressman, if I may offer, I believe a lot of the courthouses, both Federal and State across this country, are the ultimate sort of origination point for this data. We sell, because these documents are public records, we sell—16,600 divorces were granted in Harris County. We sell 930,000 pages of data every year in our office and many of those pages contain sensitive information.

Now you would imagine that most of the people purchasing this data are parties to the suit and, in fact, they are. When you go to buy a house you have to prove that you were divorced, and so forth. The title company will ask you to present this final divorce decree. So, in many cases the people coming in to buy the document are the people themselves but not in every case. And we do not and cannot control who buys this information because it is technically public record.

So, you see, we are the origination point, I think, for some of this data.

Mr. HENDRICKS. And I think you have all asked the same question. One clearinghouse to start looking at is a company called Choice Point. They specialize in buying public records and putting them into electronic database form. And I think that if all of you got your Choice Point file, it would be a real eye-opener because they get public records from all across the country so they can put together rich files on people.

Mr. COLLINS. Mr. Chairman?

Chairman SHAW. Thank you, Mr. Collins.

I would like to ask Cory a question. I know you have been working with the State of Florida university system on getting these numbers eliminated and change the ID system. Will it require different numbers for in-coming admissions only or will it take changes to currently enrolled students? And what does Florida intend to do with all of the old records that have the numbers on them?

Mr. KRAVIT. Mr. Shaw, what we would like to do is obviously all the new in-coming students would get a new number and for the old records, they want to go back as far as they can and issue new numbers for them.

They are looking at instituting a state-of-the-art directory system that would have a hidden number that nobody would ever see, which would be linked to all the other numbers, like public numbers. There would be that one number that nobody ever sees, a public number, which as a student ID number or an alumni association number, and there would also be private numbers that only people who have designated access to, like your Social Security number, would be able to view.

Chairman SHAW. Thank you.

Mr. BACARISSE. You talked about the court files and the amount of information that you have to make. I imagine that in Florida, with the sunshine law, a reporter can come to a County Clerk's desk and go through his in file and look what is in there. I mean there is absolutely no privacy left at all in that situation.

But, when you have been requested to supply a document you talked about the large expense that would go into changing over to a new system. That is one of things we are going to have to worry about because we do have unfunded mandates. Now whether this would be considered a mandate or a prohibition, I guess we would leave to the lawyers to decide. But, it seems to me that in supplying a document, and I assume it is all on microfilm, that when you print the document out you could simply put a black marker through a Social Security number. So that would not be that overly burdensome. I assume that you could also change your procedures so that Social Security numbers would not appear on public documents henceforth and that would cost you zero. I cannot think of any expense connected with that.

What would be your recommendation going forward, assuming that one of the possibilities is not Federally funding every courthouse in the country to change over?

Mr. BACARISSE. Correct. At this point, Mr. Chairman, we have calculated the cost of redaction at about $8.07 per document. And when you consider that I have 6 million Social Security numbers

in my database today, that is a cost I do not believe any local government could absorb.

Chairman SHAW. It is how much per document?

Mr. BACARISSE. Eight dollars per document. When you are talking about human staff time because you have to have——

Chairman SHAW. Is this because you have to go back and change the microfilm? I guess?

Mr. BACARISSE. You would either have to do that or we began in November of 1998 digitally imaging all of our court minutes, which are the signed orders in civil courts. So, there is some technology available today that would enable you to redact sensitive information but here again it is labor. It is labor costs. You are paying someone to go in and do that work that they had not previously had to do. So, local governments will have to figure out a way in which to handle that additional burden.

We believe that if that is going to be the case that perhaps the best way to do it is just to say at the time that the document is publicly requested, that information is redacted. It would be a little easier for us to handle administratively than just to have us go back wholesale and do this.

Of course, we also, I believe the Congress should ask States to change their laws. We are mandated by State law. The bar is mandated in the family code at least 15 times, 15 different statutes within the family code, to get that information and place it in the document.

Chairman SHAW. Let me interrupt you right there. Are you required by Federal law to take the Social Security number and place it on the public document?

Mr. BACARISSE. I am required by State statute to do that.

Chairman SHAW. State statute?

Mr. BACARISSE. Yes, sir. The bar, actually.

Chairman SHAW. In a lot of instances the Federal law would not override State law but in this instance, in that the social security number is issued by the Federal Government, we can certainly legislate that the social security number is the property of the Federal Government and then from that point forward go back and dictate how it can or cannot be used.

Mr. BACARISSE. Yes, sir. As a matter of fact, in a case affecting a parent-child relationship, a divorce with children involved, the State family code says that the Social Security numbers of the two parties in the divorce, as well as all the children, be listed in the decree, in the document.

Chairman SHAW. Is that typical? It has been 20 years since I practiced law. Is that typical?

Mr. BACARISSE. I believe these statutes have been on the books in Texas for quite a while. These are not new statutes. So, it is unfortunate that the bar is being commanded to put this information in documents which they then file with our office, which are open records. In a sense, the bar is being placed in a ticklish position of potentially placing their clients' privacy at risk, possibly.

Chairman SHAW. I think we ought to probably poll the different States to find out exactly the ways under the various State laws the use of Social Security numbers are mandated.

Mr. BACARISSE. Sir, I think you would find that a fairly high number in different States and I think you would be quite surprised.

Chairman SHAW. Well, we ought to check that out. Thank you.

Mr. BACARISSE. Thank you, Mr. Chairman.

Chairman SHAW. Thank you, Mr. Collins.

Mr. COLLINS. One last question. Supposing—do you like that word? That is a good Southern word. Supposing we pass legislation to stop the use of it today, the Social Security number. What would you do with all of the existing data that is already out there for the purpose of misuse, all these websites? If I had one of those websites and I was intending to help somebody violate the law and commit a crime, I would just simply print them out, sell them on the black market.

Mr. BACARISSE. That is a good question, Congressman. I think that as somebody said earlier, the genie is already out of the bottle and I do not know how you are going to get that cleaned up but at least from this point forward we might have some measure of protection which is greater than we do today.

There is another website that was not shown today called Ancestry.com and they have over 65 million Social Security death records. I typed in the last name of Bacarisse and put State of Texas and there are all my dead relatives and their Social Security numbers and their last known address there.

So, it is not only the living; it is the dead that can have their identities stolen.

Mr. COLLINS. I think we have ourselves a real political problem, those of you for it and those of you against it. Thank you. It has been a very interesting hearing. I appreciate each one of you being here.

[Whereupon, at 1:00 p.m., the hearing was adjourned.]

[Questions submitted from Chairman Shaw to the panel, and their responses, follow:]

Harris County District Clerk
Houston, Texas 77210–4651
July 18, 2001

The Hon. E. Clay Shaw, Jr., Chairman
Subcommittee on Social Security
B–316 Rayburn Office Building
Washington, D.C. 20515

Dear Chairman Shaw,

I was glad to testify before your Subcommittee on May 22 regarding the integrity of Social Security programs. Thank you for so carefully considering my recommendations and asking for more details.

You had five sets of questions. Here they are, with my answers:

1. You indicated that it would cost $8.07 to redact any Social Security numbers in a public document. You also indicated that you expect the overall financial impact to be similar to that of Maricopa County, AZ, whose Clerk of Court indicated he would have to hire an additional 25–30 staff and the cost could run $1 million per year. Is this additional cost based on redacting the number of pages your office certified last year, 930,000? Could you provide more detail as to why it would require that much additional staff?

The cost figure reflects our redacting the documents—usually 5–15 pages each—represented by those 930,000 pages and maintaining our current level of customer service. (Seldom does anyone wait more than an hour for a document from our office.)

Also, please note that the $8.07 cost of redaction per document estimate is based on the work's being done by our lowest-paid clerk. Assuming those 930,000 pages are in documents averaging 10 pages, that would be 93,000 documents a year redacted at a cost of $8.07 each, or $750,510 a year in salaries alone. Benefits, equipment and space costs, etc. should be added to that.

Note how closely that figure matches the $1 million a year estimate, which was arrived at using a different method. (I took Maricopa County's estimate of the number of personnel needed but used Harris County's salary and benefits numbers.)

Also, Maricopa County has advised me that the staff it uses for redaction is paid $9–10 an hour (plus benefits), so its cost would be even higher than Harris County's. Maricopa County stresses that its estimate of additional staff is very conservative and was based on only the work done at the main office, with the branch offices doing about 25 percent more.

2. The legislation introduced from this Subcommittee does not require the redaction of the Social Security numbers from documents if they are not provided to the general public. In addition, the redaction is prospective. Would this reduce the total cost you believe would be incurred?

No, it would not. We have "open courts" in this country, and that principle is vital. With few exceptions, ALL our documents may be provided to the general public. The estimate was based on the pages we already are providing the public.

Through 1998, according to the Social Security Administration, 391 million SSNs had been issued. Those SSNs are circulating now. Redacting only those Social Security numbers acquired after some future date would do little good, in my opinion.

3. You stated in your testimony that State and local governments want to work collaboratively and cooperatively with us to safeguard all our citizens' privacy. How do you suggest we "safeguard all our citizens' privacy"? What should we focus on?

Each person must be made aware that he/she has a primary responsibility for safeguarding his/her own privacy. Everyone must be educated about when and to whom confidential information should be provided and how to protect it. Shredders should be as common as televisions. Identity thieves should be pursued more enthusiastically. We must educate the public that a huge reason merchants want so much information is that they suffer so much from bad checks—and increase the penalties on people who write bad checks and make more effort to catch and prosecute them.

4. You mentioned that any laws must be effective and enforceable. What would be an enforceable law in your opinion? Is there any way, going into the future, that your operation could limit the use and access of SSNs in divorce and child support cases and still enforce the child support laws?

The current laws probably are enforceable but not very effective. Given the millions and millions of Social Security numbers floating around and available worldwide, no law will be very effective until almost all individuals decide they are going to take responsibility for protecting themselves. That won't happen if the public is convinced that all it takes to protect privacy is for Congress to pass the right law. Again, the collection of Social Security numbers and many other personal identifiers is driven by the dishonesty of hot-check artists, people who default on loans, etc. A law could fund an educational campaign that points out how the actions of a relatively few dishonest and/or irresponsible people are threatening the privacy rights of all of us.

I do not believe it would be possible to enforce child support, divisions of pension benefits, community property divisions, etc. without something like a Social Security number that by law is connected to virtually all wages, interest and dividends paid to anyone and all taxes, license fees, etc. paid by anyone. If we did not have Social Security numbers, we would have to invent them!

5. You stated that each year Harris County sells about 930,000 certified pages from family law cases. Can you explain for what purpose? How are the purchasers using the information from these pages? Can they sell this information to others?

Former spouses must have certified copies of divorce decrees and other documents to obtain Social Security benefits, pension benefits, divisions in probate court, banks and home loans and some licenses (including a marriage license after you have been divorced). Also, two associations serving apartment owners and managers purchase lists of recent felony convictions. The lists show the Social Security numbers of some but not all the felons on those lists. Clearly, the purchasers can resell the information, but my staff does not know of anyone obtaining numbers simply to resell the numbers.

I hope these responses are helpful. If you need more information, do not hesitate to contact me.

Sincerely,

Charles Bacarisse
District Clerk

Privacy Times
Washington DC 20009
July 19, 2001

The Honorable E. Clay Shaw, Chairman
House Ways & Means Committee
Subcommittee On Social Security
U.S. House of Representatives

Dear Mr. Shaw:

Thank you for this opportunity to comment on the bill; unfortunately, other obligations and deadlines have significantly limited the amount of time I have available to work on this. But I hope I will be freer in the near future to help as your bill evolves.

Question 1. In your testimony you listed 4 goals that Social Security number privacy legislation should achieve. As you know, members of this Subcommittee recently introduced H.R. 2036, bipartisan legislation restricting the sale and display of the Social Security number in the public and private sectors. I am interested in your thoughts as to the legislation.

First, does it accomplish these goals? For example, does it go far enough in restricting the sale and display of Social Security numbers by Federal, State and local governments? If not, what do you recommend?

Second, the legislation provides for a prohibition of an individual's Social Security number from appearing on their driver's license. Was this sufficient?

Third, it removes the Social Security number from the credit header and placed it in the credit report. Your comment?

Fourth, what standards should we set for all organizations that collect and maintain Social Security numbers?

(1) HR 2036 substantially advances my stated goals of

- Ban the sale of SSNs by the private sector, particularly as part of credit headers.
- Prohibit the sale and display of SSNs by Federal, State and local governments.
- If not an outright ban on the use of SSNs as a driver's license number, then mandate that DMVs can only use the SSN if the driver opts in, as is currently practiced in the District of Columbia.

However, it does not address my 4th goal, which is the standard your bill should include for any organizations that collect and/or maintain SSNs. The standard is straight from the U.S. Privacy Act. A private right of action should apply to violations of this standard, and to any section of the bill.

- Place a duty on all organizations that collect and maintain SSNs to "establish appropriate administration, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." (This standard is from the U.S. Privacy Act of 1974)

In addition to drivers licenses, all organizations, particularly universities, should be barred from displaying SSNs, like when they post students' grades, or on organizational ID cards, like student or employee ID.

As recommended by the Privacy Protection Study Commission (PPSC), the legislation should create an independent privacy oversight office, as oversight and enforcement will be needed. Moreover, the legislation must formally require that any future legislative proposals for expanding uses of SSNs be brought before the Subcommittee and its counterpart in the Senate.

Question 2. You mentioned that the sale of Social Security numbers and the coercion of individuals to needlessly give their numbers should be banned, with few exceptions. What exceptions do you think would be appropriate and why? How are Social Security numbers protected in these exception cases?

(2) I don't favor exceptions, though it is possible that some entities could come up with exceptions to which few people would disagree. I will consider exceptions as they are proposed.

Question 3. In other testimony before the Subcommittee, the use of Social Security numbers for child support cases was highlighted. How do you deal with an issue like this where the welfare of the child may depend on the ability to find the father, and that rests with knowledge of his Social Security number? Is this a legitimate reason for government to use the Social Security number?

(3) The Child Support system has been exempted from virtually every privacy rule, yet they continue to complain they still do not have enough tools. I assume they will be exempted from most SSN restrictions. They should still be responsible for protecting the security of the number, and guard against unauthorized use. Given the many exceptions they enjoy, I think the real problem is the nature and design of the child support system and some of the people who operate it.

Question 4. In your testimony, you mentioned corporations that provide privacy protections for consumers such as the wireless communications industry. What are they doing to provide such protections?

(4) The wireless industry sees privacy as integral to the success of M-Commerce, and therefore has petitioned the Federal Communications Commission for a strong, opt-in privacy standard for the use of consumer location data. Another important new development is the single-use or disposable credit card number which is only good for one transaction and therefore becomes worthless. American Express, MBNA and Discover offer disposable credit card numbers to online customers. A company called PrivaSys to which I consult is creating a plastic credit card with disposable number functionality.

Question 5. Last session, Congress passed the Gramm-Leach-Bliley Act. What, if any, shortfalls, does it have in protecting Social Security numbers? Once begun, do you think consumers will feel confident these new protections in the financial sector are adequate?

(5) For starters, Gramm-Leach-Bliley failed to put a strong enough duty on banks to safeguard SSNs, and to create a private right of action against banks that violated that duty. The negative public response to the GLB customer notice already has shown that GLB is wholly inadequate to protect consumer privacy. However, it a perverse sort of way it has advanced privacy by helping to educate consumers how poorly their financial privacy is protected.

Question 6. Mr. Bacarisse stated in his testimony that Harris County and its taxpayers would bear a financial burden if they had to hire additional staff to redact the Social Security number from documents that they receive in their office. Are you concerned about the cost that will be borne by the taxpayers?

Do you have any suggestions for these governmental agencies in ways to handle the redaction of Social Security numbers?

(6) It is not practical to require every court, State and/or local government to redact SSNs from every piece of paper that is publicly available. However, the legislation should basically override every rule that requires individuals' SSNs to provided as part of a record that will be publicly available. Second, create a process by which individuals can have their SSNs redacted from paper records, like people who have been through divorces, bankruptcies, etc. Third, if SSNs are stored electronically and are publicly available, then automated software programs could use "find and replace" functions to redact SSNs in a non-burdensome and low-cost way.

Question 7. You stated that Social Security numbers were not widely used in the private sector prior in 1976. You stated that TRW (now Experian), a major credit bureau, did not use it as its main identifier for credit reports. Assuming that credit bureaus like TRW did not have difficulty identifying individuals in 1976, can you tell us why the Social Security number is so critical now?

(7) Organizations claim the SSN is critical to identifying someone because so many of them are accustomed to using it. But the reality is that information technology allows many alternatives to SSNs, including PINs and passwords. A positive result of this legislation will be to wean organizations from their reliance on SSNs. This will not happen overnight, but will be an evolutionary process.

Question 8. In their testimony, Mr. Dugan, Mr. Plesser and Ms. Leroy all mentioned the powerful consumer benefits to be derived from the use of an individual's Social Security number as a common unique identifier. What is your response?

(8) The Dugan/Plesser arguments about "powerful consumer benefits" because of the SSN are largely specious. These same "benefits" which they proclaim remain after this legislation puts the appropriate restrictions on their clients from exploiting SSNs without consumer consent. It's simply a matter of adapting systems so they don't rely on SSNs. In the financial world, it's already mandated that banks use SSNs, so that won't change current practice.

Question 9. Would you agree with Mr. Plesser's testimony that the best means of preventing identity fraud is through use of personal identifying data like the Social Security number, often matched through individual reference services?

(9) No, Mr. Plesser has it backwards. The credit reporting agencies' over-reliance on SSNs has facilitated fraud. Identity thieves know that as long as they have an innocent victim's SSN, the credit reporting agencies' systems will tolerate different first and last names, different addresses, even different States. Moreover, some of the IRSG group members do not provide one of the most fundamental anti-fraud solutions: easy consumer access to their own data.

I'd look forward to working with the subcommittee.

Yours truly,

Evan Hendricks
Editor/Publisher

Financial Services Coordinating Council
Washington, D.C. 20004

1. The deterrence and prevention of fraud is an on-going effort of the financial services industry. Banks, insurance companies, and securities firms rely on information available from both public and private sources—with embedded social security numbers (SSN) to ensure correct identification—to check for inconsistencies that may suggest the occurrence of fraud or identity theft. Just as with any other crime in our society, best efforts will likely not be successful in eliminating every occurrence of a criminal activity. Elimination of financial fraud and abuse involving SSNs is our goal. While that is an ambitious goal, the financial services industry will use every tool available to us in order to limit such crimes as much as possible. The SSN is one of those tools, and it is one of the most valuable. **[See my comments previously sent.]** We are unable to comment on the specifics of this matter because we do not have enough facts concerning how this particular identity theft may have been perpetrated. However, financial institutions are required under section 501 of the Gramm-Leach-Bliley Act to implement policies and procedures that protect the security and confidentiality of customer information. Federal and state agencies have, or are in the process of, promulgating guidelines and regulations that financial institutions must follow to ensure that customer information is not misused by fraudsters. In this regard, the federal banking agencies recently issued advisory letters which specifically focused on the protection of customer information against identity theft. We believe that financial institutions are well along in the process of implementing systems and procedures that bolster their ability to prevent and detect identity theft perpetrated through the use of social security numbers or otherwise.

2. Financial institutions do not sell social security numbers except indirectly as incidental to normal business transactions, such as the sale of portfolio and securitization. The Gramm-Leach-Bliley Act (GLBA) and the federal and state laws and regulations which have been adopted to implement the GLBA already provide very specific rules and limits on the ability of financial institutions to disclose nonpublic personal information (NPI)—including SSNs—as well as to redisclose and reuse SSNs. As a result, additional restrictions on financial institutions' disclosures of SSNs are unnecessary and would conflict with these existing laws.

More specifically, GLBA Section 502(c) provides that a nonaffiliated third party which receives NPI from a financial institution may not disclose such information to another nonaffiliated third party unless such disclosure would be lawful if made directly by the financial institution. Accordingly, an unrelated third party which receives a social security number from a financial institution is subject to the same rules to which the financial institution is subject in connection with any redisclosure of the social security number. The federal banking regulators and the state insurance regulators elaborate on this limitation in their respective rules to implement the GLBA. They provide very specific guidance with respect to the use and disclosure of NPI, including social security numbers, both by financial institutions and by nonaffiliated third parties which receive NPI from financial institutions. (GLBA Banking Regulators' Rules Section _____.11 and National Association of Insurance Commissioners (NAIC) Privacy of Consumer Financial and Health Information Regulation Section 12.)

In our testimony we expressed the concern that a prohibition on the direct or indirect sale of social security numbers could have the unintended consequence of being construed to apply to usual and customary business activities such as the sale of assets among financial institutions or the sale of financial institutions. Such a prohi-

bition necessarily would be of grave concern to financial institutions. No inference should be drawn from our testimony that financial institutions sell social security numbers as free-standing commodities.

Finally, any restrictions on financial institutions' use or disclosure of social security numbers beyond those already imposed under the GLBA and related federal and state laws and regulations are likely to have further unintended consequences and to impair financial institutions' ability to combat fraud and identity theft and to provide customer service for the reasons set forth in our testimony.

3. Financial institutions use a variety of public records, including bankruptcy records and records involving real estate liens. They also use criminal and fraud detection databases, such as the National Fraud Center database, which are developed using public records. Access to information in public records, including social security numbers, is important to financial institutions' efforts to uncover fraud and identity theft, to verify customers opening new accounts, to maintain internal security operations, and to make sound credit and other financial product determinations. It is also important for third parties such as credit bureaus to continue to have access to this information as well. Financial institutions rely upon these third parties to prevent and detect fraud and identity theft.

We believe that legislation to address identity theft should be carefully targeted to that particular problem and should avoid restrictions on normal and beneficial uses of social security numbers which actually serve to protect consumers against fraud and identity theft and which improve customer service. The type of fraudulent activity with which the Subcommittee is concerned does not arise from the aforementioned uses of public records. We are concerned that broad restrictions on the use of social security numbers could have the opposite effect from that intended by the Subcommittee and could result in making it easier for individuals' identities to be stolen.

4. For the reasons stated above in response to question # 3, we believe that legislative efforts should be carefully targeted to address the specific fraudulent activity which is of concern and should avoid normal and beneficial uses of social security numbers.

5. We recognize that there are circumstances under which the use of social security numbers could be harmful. Identity theft associated with the misuse of social security numbers is a prime example. There are already some existing laws which address identity theft. Stealing someone's identity is punishable by civil and criminal penalties under 18 U.S.C. δ 1028 and the GLBA makes it a federal crime to obtain customer information of a financial institution through fraudulent or deceptive means (so-called "pretext calling). 15 U.S.C. §§ 6821 et seq. As noted above in our responses to questions #'s 3 and 4, we believe that legislation to restrict use of social security numbers should be carefully crafted to address the problems of identity theft not currently addressed in existing law.

6. As stated in our response to question #2, we believe that the GLBA and the federal and state laws and regulations adopted to implement the GLBA already impose comprehensive restrictions on financial institutions' disclosure and reuse of social security numbers. These laws also address the circumstances under which a consumer must be given the opportunity to direct that his or her NPI, including a social security number, shall not be disclosed by a financial institution. Therefore, an additional requirement that financial institutions obtain consent prior to re-use or re-disclosure would not only give rise to a significant administrative problems and considerable expense, but would be in conflict with existing law governing financial institutions on the federal and state levels. Any restriction on access to social security numbers in public documents would give rise to the concerns addressed in our response to question #3.

7. We believe that existing federal and state law and regulations adequately and appropriately govern financial institutions' use and disclosure of social security numbers as expressed above and as stated in our testimony.

Sincerely,

John C. Dugan
Partner, Covington & Burling

Individual Reference Services Group
July 19, 2001

Subsequent to the IRSG testimony, the IRSG has agreed not to further pursue its appeal challenging the FTC's treatment of credit header information under the Gramm-Leach-Bliley Act. As a result, the IRSG is now facing a world of "regulated

credit headers." Therefore, the IRSG is in the process of evaluating its self-regulatory program, which was developed to respond to a pre-GLB world.

The answers we are providing to you are based on the IRSG Principles as applied to date. To the extent that this self-regulatory approach changes, we will inform the subcommittee.

1. You indicated in your testimony that the Individual Reference Service Group's (IRSG) principles focus on non-public information about an individual neither available to the general public nor obtained from a public record. Is it correct then to say that if the Social Security number you obtained from credit headers was obtained originally from public records, these principles would not apply?

No, this is not accurate. All information obtained from a credit header would be deemed subject to the IRSG Principles.

2. Not many people know of the IRSG industry and what it does. You indicated that your members are committed to educating the public about their database services. Shouldn't they know what information you maintain and their access and rights to the use of that information? What steps have IRSG members taken to educate the public?

The IRSG has undertaken educational efforts to ensure that the public is aware of its self-regulatory Principles governing the dissemination and use of personal data. The IRSG Web site serves as the cornerstone of these education efforts. This site enables visitors to read the IRSG's self-regulatory Principles, and provides links to each of the member companies' privacy policies, which discuss the individual companies' information practices. The member companies' Web sites themselves also help educate the public about the commitment these companies have made to responsible information use. For example, ChoicePoint provides its users with IRSG FAQs. See <<http://www.dbtonline.com/irsg-faq.asp>> Similarly, Acxiom educates the public by informing consumers at its Web site "what every consumer should know" about its privacy. See <<www.acxiom.com/DisplayMain/0,1494,USA~en~777~938~0~0,00.html>>. In addition, several member companies, such as LexisNexis, produce educational brochures, targeted at both employees and members of the public, that explain the IRSG self-regulatory Principles. See attached Exhibit 1. Finally, the FTC Web site maintains various information about the IRSG.

3. You indicated in your testimony that you oppose legislation that would ban the purchase and sale of Social Security numbers by businesses that have legitimate business purposes to use the number. Could you elaborate on your objections? For example, what is a legitimate business purpose?

Any legislation that would restrict the use of SSNs to match records or allow retrieval of location information for an individual by searchers who already know that SSN would seriously undermine the broad range of important and socially beneficial activities by government, businesses and non-profit users that rely upon the use (but not display) of a known SSN obtained from a commercial database. For example, it would undermine: efforts to detect fraud and combat identity theft; child support enforcement; efforts to locate pension fund beneficiaries; and non-profit health services' efforts to locate blood, bone marrow, and organ donors.

Legitimate business purposes also include: the facilitation of credit checks or background checks of employees, prospective employees, and volunteers; the retrieval of information from, or by other businesses, commercial enterprises, governmental agencies or private non-profit organizations; and identifying or locating individuals or verifying their identities, as well as verifying the accuracy of information identifying individuals. These purposes should not include the provision of SSNs on the Internet to the general public.

4. You testified about the uses of individual reference information. What role does the Social Security number play in obtaining this information? Is there no other way for your group to obtain the same information?

SSNs are used in our industry as a glue to ensure the accuracy of information as well as to ensure that information is attributed to the correct individual. Although there are other ways to match information, our experience indicates that SSNs are the best tool for indexing and organizing data accurately.

5. You stated that restricting the use of the Social Security number to indexing and verification would result in more rather than less identity theft. What studies do you have to support this?

This statement is based upon our members' experiences in furnishing anti-theft products to their clients. Our members' databases are used by department stores, banks, insurance companies, utility companies and governmental entities to detect and stop identity theft. Without SSNs, our members' experience has been that it is more difficult to detect perpetrators of fraud who use another's identity to illegally obtain products, services, or money.

6. You indicated that if a company receiving information from one of your members did not comply with the principles for resale, they risked losing access to the data. Have any companies been found to be in non-compliance so that their access to members' data has been cut off? How would that work? If I am found to be in non-compliance with one member, would all members of the IRSG be prohibited from supplying me data? How could I correct my non-compliance?

The IRSG Principles were designed so that no IRSG suppliers would give information to companies in contravention to the Principles. That is, the signatories to these Principles require by contract that all companies buying non-public data from them for resale abide by the Principles then in effect. That has been the dominant practice. Any signatory company may be responsible under existing federal and state law on deceptive practices if the company fails to live up to these Principles. In addition, every IRSG member company is subject to an annual outside assurance review by qualified independent professionals. Information is provided only to IRSG member companies that successfully complete the annual assurance review.

7. You indicated that each member undergoes independent assurance reviews. Are copies of the reviews provided to the Federal Trade Commission? If not, what do you provide the Federal Trade Commission regarding the results of these independent reviews?

Each company is required to submit to the IRSG coordinator a copy of the letter it has received from an independent assessor certifying compliance with the Principles. We do not have back-up documentation of the assurance reviews, other than the letter indicating successful compliance. We have attached to this document examples of assurance letters. See attached Exhibit 2. We post, on an annual basis, a statement indicating successful completion of assurance reviews, and the names of the independent assessors that performed the assurances. See << www.irsg.org/html/irsg__assessment__letters__2000.htm>> for 2000 assessment letters. In addition, the criteria used for the assessments are posted on the IRSG Web site and the fact that these criteria are publicly available is referenced in the assessment letter.

8. You mentioned that companies that buy information from your members must sign a contract requiring them to abide by your principles. Who monitors compliance with the principles among your members' customers?

The procedures vary from company to company, but compliance is monitored through the annual audit.

9. You stated that if your members' customers don't comply with your principles, they risk losing access to the data they need. Isn't there a financial incentive for your members to overlook violations of the group's principles, since they would lose a customer and lose profits?

IRSG member companies may be responsible under existing federal and state law on deceptive practices if the company fails to live up to the IRSG Principles then in effect. Both the FTC and state AGs have authority to prosecute such violations.

10. Recently an article appeared in the Washington Post detailing how individuals would provide false information to on-line data brokers in order to obtain personal data. How do your member companies prevent somebody from purchasing personal data for illegal purposes? In other words, how do your member companies determine what is a legitimate request?

Principle V of the IRSG Principles sets forth the criteria for distribution of non-public information. The nature of non-public information being requested and the intended uses of such information determine what access a subscriber has to information. Companies that offer non-public information without restriction of its contents only provide such information to qualified subscribers who satisfy the requisite conditions. Member companies undertake extensive screening processes to pre-qualify users of these products. Such measures include positive proof of identification, site visits by account representatives or independent verification of customers' name and affiliation. Companies also have guidelines for acceptable uses of information. Where a new use is contemplated, the new use is reviewed to determine whether this use comports with the Principles.

11. Do you have any statistics that support your assertion that reference services reduce credit card identity fraud?

No. We do, however, have anecdotal evidence from law enforcement and our members' customers that supports this assertion.

Sincerely,

Ronald L. Plesser

Pension Benefit Information
Tiburon, California 94920
July 24, 2001

Honorable E. Clay Shaw, Jr.
Chairman of the Subcommittee On Social Security
House of Representatives
Washington, DC 20515

RE: Testimony before Subcommittee On May 22, 2001—Identity Theft issues

It was a privilege to testify before your Subcommittee and it is very gratifying to know that someone is listening. Thank you for this opportunity to respond to the questions you pose regarding privacy and Social Security Numbers.

Question 1. Regarding the information we obtain from pension plans: When we receive information from a pension fund administrator or plan sponsor, our written policy is to only utilize the information for the purposes for which the data was collected. In other words, we pledge to do the job our client expects, and at no time do we re-disclose the information. We share no information outside of the client relationship.

Response. We do keep the information we collect in our system, because over time, we receive numerous calls from participants who want to update their address for a second or third time. In effect, we become an "update" agent for people who were once lost, and want to stay "found". The information we store is available only to privileged users in the company with proper passwords, and every record entered or altered is encoded with the users name/date/time. Records cannot be printed from data entry screens.

Question 2. Each day in our business we are keenly aware of the importance of an individual's Social Security Number. It is a very vital pointer to an individual, and it is unique in that it points to only one person. I believe strongly that there should be restrictions on the use of the SSN, and it should be predicated upon the intent of the user, and oversight might be an important key. By way of example, let me explain our relationship with the IRS. We presently utilize the IRS letter-forwarding service, for the difficult cases we encounter—people that cannot be found any other way. We submit a letter to the IRS and pay a fee to have the IRS forward the letter to the person who owns the SSN that we submit for the search.

Response. The IRS uses the utmost care in investigating the users of this service, and each user must pass the litmus test: the location of the individual must be for the benefit of the individual. We have been utilizing this IRS program for over 11 years, month in and month out. This opportunity to use the IRS resources to locate people is available to our company because we pass the test of legitimacy—a test administered by the IRS. I am suggesting that the personal data be restricted, and that users be bonded, submit documentation on procedures, subject themselves to outside audit if necessary, and bear the burden of proving the need to know. Legitimate business can pass these tests.

Restrictions on usage of personal data, I believe, should be governed by the opportunity for personal benefit for the individual. In the case of restoring pension benefits to an individual, I believe that the personal benefit is real and tangible, because at one time the individual chose to enter the plan. By making a conscious choice to participate in the plan certainly underscores the benefits. This logic can be used with bank and brokerage accounts, insurance policies, and other such vehicles of personal benefit as well. For the record, may I also include class action lawsuits. We have been involved with searching for beneficiaries of class actions, and the benefits are obvious.

Lately, many millions of dollars have been spent in creating and disseminating privacy notices to individuals. These have largely been thrown away and ignored, because the public does not generally perceive the banks and insurance companies as the agents of privacy breaches. Perhaps they contribute to the "junk mail" we all receive, but not identity theft. The **legitimate exchange of data** that was effectively stopped in its tracks by the FTC interpretation of Title V under the recent GLB Act was not the source of harm to the greater public. The real danger has been the proliferation of the heretofore unregulated internet, and its data collection and dissemination ethics. There have always been scam artists, pickpockets, and savvy schemers that could invade a person's private life, but now the internet has made their criminal endeavors a lot easier, and more removed from the light of day. Additionally, the manner in which credit is extended to the wrong individuals is shocking. Surely there must be some checks and balances before a person can receive a

new credit card with a stolen identity? We all receive multiple offers each week for yet another . . . must have . . . credit card. I believe the credit grantors are not suffering enough pain to stop this cycle, and that once they tighten up the credit-granting process, at their own expense, theft identity will begin to diminish, and thieves will move on to more lucrative avenues. As long as a criminal can open up several credit accounts, wrestle into bank accounts, and juggle multiple identities, identity theft will continue and flourish, despite the new privacy laws.

Whatever the punishment might be for misusing an individual's SSN, it has not been a deterrent to date, and I feel it has become even easier to commit such crimes, via the internet. Credit scam factories, versus individual small-time thieves present different problems, and I feel it is the responsibility of the criminal justice system to provide adequate investigation and punishment. Certainly restitution to the parties harmed must be enacted, and credit grantors must step up to the plate if they have allowed "easy credit" to criminals.

Question 3. Regarding prior consent for using an SSN to look for a person, may I say that YES, this could be one way in which to operate our business. An employer could, at hiring date, or entry into the pension plan, require a release from each individual. And then file the release away somewhere, in case it is needed. And then, better be able to find it on the day the person comes up missing. (What about all the millions of people that have not signed a consent form at this time, and are missing now—or may turn up to be missing later?) Because of a crackdown on the criminal uses of SSNs, the burden of privacy will now move to employers and employee benefit programs. Not only will the employers/plan sponsors have the task of proper enrollment forms, vesting requirements, investment protocols, plan document construction, notification procedures, ERISA requirements, DOL reporting requirements—you see my point here? The benefits industry presently operates under so much legal pressure, that it will be construed as burdensome to put yet another set of documents under their purvey. And, like all other aspects of business, benefits departments are moving to a paperless environment. For a company like General Motors, this would involve more than 300,000 pieces of paper. How do you file them? Where do you keep them? Do they stay in Detroit, or do they go out to the various operating plants? What if they sell a division? Where do the forms go now? How do you find all the forms for the division being sold?

Response. I think, as stated above, that it is IMPLIED in the relationship of plan sponsor/participant that an individual who enrolls in a pension plan would likewise want to receive the benefits covered under the plan. Why should they have to "opt-in" for a concept that is clearly understood? If an SSN must be utilized in the process of hiring a person, paying a person, withholding taxes from a person, filing tax documents, and providing health care and retirement benefits, then so be it. There are surely numerous justifications for utilizing an SSN. Note here that under the GLB, one of the exemptions is for "employers" use. When queried, the FTC informed me that this was for hiring individuals, and doing a background check as part of pre-employment investigations. Ask any man-on-the-street if he would rather have his employer use his SSN for an investigation into his personal credit history, or for returning vested pension benefits!

Question 4. After approximately 13 years of locating individuals, there is no better resource than the SSN for searching purposes. Names are never constants. My own uncle legally changed his first name (after Grandma died) because he hated it. Women change from maiden name to married name, back to maiden name. Nicknames are used all the time, so Anthony becomes Tony to all who know him. Worse, birth dates are the most confusing pointers we see as far as information for searching. Pension plans often capture only mm/yy for actuarial purposes, and if the full mm/dd/yy is collected, it is not always entered correctly into the system. When we cannot find a match, is it the month that is wrong? Or is it the year? For John Johnson, one might find 1,000 men with that name, all born in March, 1945. To eliminate the use of SSN as an identifier performs a disservice to the pension plans as well. If you wanted to return $10,000 of pension benefits to someone, wouldn't it be prudent to make sure you have the right John Johnson? John Johnson with the right name and date of birth could be the absolute wrong person unless the SSN is utilized.

Question 5. Regarding the restriction of commercial databases, I do not believe that the culprit is the commercial data base industry (or information services, to use another name). What they have is valuable, vital information, which must be treated with care. There are legitimate, beneficial purposes to have access to the information in these databases. Because criminals use information that is either obtained from or coincidentally resides in these databases does not warrant a complete shutdown of the process. I very vividly recall the testimony before the Committee from the two poor souls whose identity was stolen: they were first victims of theft.

Someone had stolen a gym bag with a wallet in it, and another person snooped into a medical file and lifted information. The tragedy is that the two thieves were able to obtain credit with the stolen identities. How can this be? What about mother's maiden name? What about previous two addresses? What about the city of birth? These kinds of questions can easily be answered by the REAL person, and a would-be thief would have a tough time with the same questions. I am suggesting that credit is a privilege that requires authentication beyond the measures that are presently in place.

Lastly, regarding a move away from Social Security Numbers, I truly believe that matching on other personal items will cause more confusion and lead to more problems, because of the reasons I presented earlier; names and birth dates are not unique. SSNs paired with names are unique, and provide the best data. The data needs protection and oversight.

At PBI, my company, we want to do the best job we can in locating people who have pension benefits left with a former employer. We need accurate data from the pension plan, and likewise, accurate and reliable data to guide us in our search.

Thank you for this chance to respond. I would eagerly welcome the opportunity to continue a dialogue on these troublesome issues, and the future legislation that can best serve and protect your constituents at the same time. Legitimate business to business relationships must be preserved for the greater benefit of all, and these same businesses should be included in the solution.

Sincerely,

Paula LeRoy
President

U.S. Public Interest Research Group
Washington, DC 20003
July 20, 2001

The Honorable Clay Shaw
Chairman, Subcommittee on Social Security
U.S. House of Representatives
Washington, DC 20515

RE: Additional questions to witnesses on HR 2036

Dear Mr. Chairman,

Thank you for the opportunity to testify on Social Security Number misuse. Please note that I concur in full with any more detailed comments of my colleagues, Marc Rotenberg of EPIC and Evan Hendricks of Privacy Times. I do not repeat your questions below, but answer them in the order requested in your letter to me:

Question 1. In their testimony, Mr. Dugan, Mr. Plesser and Ms. Leroy all mentioned the powerful consumer benefits to be derived from the use of an individual's Social Security number as a common unique identifier. What is your response?

I disagree with the statement by witnesses Dugan, Plesser and Leroy that powerful consumer benefits accrue from using SSNs as supposedly unique identifiers. In fact, the sloppy use of SSNs by financial institutions and consumer reporting agencies (along with the ease of obtaining these numbers) has paradoxically led both to credit denials due to mistakes in credit reports (where SSNs do not provide enough of a match for consumers to keep their credit reports accurate) and also to the growing problem of identity theft (where the ease of availability of SSNs makes it easy for thieves to obtain credit in others' names). As I point out below in my answer to Question 6, numerous flawed practices by both credit repositories and creditors lead to identity theft and inaccuracies in credit reports.

Question 2. You strongly support enactment of overarching privacy legislation applicable to all business. You also recommend the extension of a strong anti-coercion credit header loophole. As you are aware, we recently introduced H.R. 2036, a comprehensive bill aimed at restricting access by the general public to the Social Security number in both the public and private sectors. I would appreciate your views as to what parts of the legislation you support and where you think we need to modify the legislation?

While U.S. privacy legislation has responded to needs as risks have been identified, the growing convergence of industry sectors suggests that one law applicable to all transactions, if strong enough, may be a useful solution. Until we can pass such an over-arching law, which is a politically complex endeavor, we should continue to attempt to pass positive laws that are achievable in the current political context. I believe that your bill, HR 2036, has many positive attributes. Of the cur-

rent SSN protection proposals, it has two extremely laudable provisions that are not matched in any other SSN bills: its strong anti-coercion provision and its credit header loophole provision (of course, Rep. Kleckza, an original co-sponsor of HR 2036, does have a separate, broader credit header bill that includes further restrictions, but these measures are outside the subcommittee's jurisdiction).

HR 2036 could be improved by narrowing its exceptions, as EPIC points out in detail in its responses. I concur with EPIC. In addition, the bill could be dramatically strengthened and improved by adding a private right of action for data subjects.

Question 3. You stated in your testimony that you support technology forcing time limits on private uses of Social Security numbers so that firms are forced to develop more accurate alternatives that do enable secondary use of Social Security numbers and potential theft. Can you expound on this?

My point in recommending technology-forcing time limits is simple. If the committee, in its wisdom, retains exceptions to the general ban on the use of SSNs in the private sector, for example, it should not make those exceptions permanent. The only way to wean industry from its over-reliance on the SSN is to set sunsets on its uses (or, what I called in my testimony, "technology-forcing time limits"). By "technology-forcing," I am not suggesting that the committee need develop any technical language or technical solutions. All the committee needs to do is set a reasonably-short sunset or deadline on further uses of SSNs, if it is reluctant to, for example, immediately ban private uses on passage. Industries would then be forced to finally develop their own technologies to solve the problem of working without SSNs.

Question 4. You stated in your testimony that you oppose the use of Social Security numbers as student identification or health record identifier. You suggested these uses should be phased-out with the enactment of trigger-based, sunset regulation prohibiting the use of Social Security numbers in the private sector. Can you elaborate on this?

Your goal should be to put the SSN genie back in the bottle. Again, if you face political pressure to grant exceptions to your general rule that the use of SSNs as health, college or other identifiers is allowed in your final bill, you should force industry to develop more accurate identifiers that do not invade privacy or violate the original uses of the SSN. Motor vehicle departments have demonstrated that alternatives to SSNs can be developed easily. There is no reason not to expect schools and hospitals to do the same. The use of the SSN in health-related situations is especially problematic, since the misuse of the SSN acts as a key for significant privacy invasions.

Question 5. You stated that you have used pretexts to prove how easy it is to get personal information. Can you elaborate on what pretexts you used and what information you got?

My use of pretexts has been on the Internet, on behalf of reporters, with the permission of the data subject. We have routinely visited information broker sites and used the pretext that the data subject "owed me money" to convince the broker that we met its so-called "standards" to obtain SSNs. We then used the SSN to obtain credit in the data subject's name and commit identity theft. Of course, high school dropouts can also do this, as other witnesses pointed out at the hearing, suggesting strongly that SSNs need to be taken out of circulation. The ease of obtaining SSNs, of course, is only part of the problem. As I point out in my answer to Question 6, poor practices by creditors and credit bureau repositories then abet the problem.

Question 6. Would you agree with Mr. Plesser's testimony that the best means of preventing identity fraud is through use of personal identifying data like the Social Security number, often matched through individual reference services?

I disagree with Mr. Plesser that individual reference services using SSNs will somehow prevent identity theft. The three national credit reporting bureaus (founders and members of the IRSG, at least until recently) have used SSNs for years as an identifier: the result has been more errors and more identity theft. See PIRG's full platform to prevent identity theft at http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/. Taking SSNs out of credit headers and out of circulation, as the District Court's decision upholding the Gramm-Leach-Bliley rules does in IRSG and Trans Union vs. FTC (District of the District of Columbia, 30 April 01) is the better way to prevent identity theft.

Thank you again for the opportunity to testify before the committee. We look forward to working with you on final passage of your important legislation to protect Social Security Numbers.

Sincerely yours,

ED MIERZWINSKI
Consumer Program Director

[Submissions for the record follow:]

Statement of David K. Byers, Conference of State Court Administrators, Arlington, Virginia

Mr. Chairman and Members of the Subcommittee,

The Conference of State Court Administrators (COSCA) is pleased to submit this statement for the record as the subcommittee examines the issue of protecting privacy and preventing the misuse of Social Security numbers (SSNs).

SUMMARY

Mr. Chairman, social security numbers are pervasive in state court documents and procedures. The testimony that follows gives the subcommittee numerous examples of how we use SSNs in day-to-day court proceedings. For example, we use SSNs to identify parties to a case, i.e. to determine whether John Smith 1 is different from John Smith 2. We also use SSNs to collect fines and restitution. In addition, many SSNs appear in the public record in many types of court cases including, but not limited to, bankruptcy, divorce and child support determination cases. My testimony also details the federal requirements imposed on us to collect SSNs for various reasons, for example, to track deadbeat parents.

Mr. Chairman and members of the subcommittee, we are greatly concerned about any effort by this Congress to require us to redact or expunge social security numbers that appear in public records. We feel that this type of requirement would impose an unfunded mandate on state courts in this country. The cost to fulfill this requirement would be high because many SSNs appear in paper documents as well as other hard-to-redact microfilm/microfiche.

At a minimum, we would ask you to wait to take action on this matter until you examine the results of an ongoing GAO study on this issue in which we have participated.

ABOUT COSCA

Before I begin my remarks, I would like to provide some background on our group and our membership. I submit this testimony as the current President of the Conference of State Court Administrators (COSCA). COSCA was organized in 1953 and is dedicated to the improvement of state court systems. Its membership consists of the principal court administrative officer in each of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the Territories of American Samoa, Guam, and the Virgin Islands. A state court administrator implements policy and programs for a statewide judicial system. COSCA is a nonprofit corporation endeavoring to increase the efficiency and fairness of the nation's state court systems. As you know, state courts handle 97% of all judicial proceedings in the country. The purposes of COSCA are:

- To encourage the formulation of fundamental policies, principles, and standards for state court administration;
- To facilitate cooperation, consultation, and exchange of information by and among national, state, and local offices and organizations directly concerned with court administration;
- To foster the utilization of the principles and techniques of modern management in the field of judicial administration; and
- To improve administrative practices and procedures and to increase the efficiency and effectiveness of all courts.

STATE COURTS' INTEREST IN COLLECTING AND USING SOCIAL SECURITY NUMBERS

Why is this question of concern to state courts? Why do state courts need to require parties to provide their social security numbers in the course of state court litigation?

Identification of parties. A growing number of court systems are using case management information systems in which an individual's name, address, and telephone number are entered once, regardless of the number of cases in which the person is a party. The advantage of these systems is to be able to update an address or telephone number for all cases in which the person is a party by a single computer entry. Social security numbers provide a unique identifier by which court personnel can determine whether the current "John Smith" is the same person as a previous "John Smith" who appeared in an earlier case.

Courts have often used social security numbers to identify criminal defendants as well as parties to civil cases. In the future, persons accused of crime will be identified by automated fingerprint identification systems (AFIS) which scan fingerprints

and classify them electronically. The primary future need for social security numbers as a means to identify individuals will therefore be in civil, not criminal, litigation.

Collection of fees, fines and restitution by courts. Social security numbers are the universal personal identifier for credit references, tax collection, and commercial transactions.

When courts give a criminal defendant an opportunity to pay an assessment resulting from a criminal infraction in periodic payments, the court needs to be able to function as a collection agency. Having the convicted person's social security number is necessary for use of state tax intercept programs (in which a debt to the state is deducted from a taxpayer's state income tax refund) and other collection activities. Some states use additional means to enforce criminal fines and restitution orders, such as denial of motor vehicle registration; social security numbers are often used for these purposes as well.

Creation of jury pools and payment of jurors. Social security numbers are a necessary part of the process by which multiple lists (for instance, registered voters and registered drivers) are merged by computer programs to eliminate duplicate records for individual citizens in the creation of master source lists from which citizens are selected at random for jury duty. Duplicate records double an individual's chance of being called for jury duty and reduce the representativeness of jury panels. Some courts use social security numbers to pay jurors as well.

Making payments to vendors. Social security numbers are used as vendor identification numbers to keep track of individuals providing services to courts and to report their income to state and federal taxing authorities.

Facilitating the collection of judgments by creditors and government agencies. Courts are not the only entities that need to collect judgements. Judgment creditors need social security numbers to locate a judgment debtor's assets and levy upon them. Courts often require that the judgment debtor make this information available without requiring separate discovery proceedings that lengthen the collection process and increase its costs. Federal law now requires state courts to place the parties' social security numbers in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgements in order to facilitate the collection of child support. On October 1, 1999, that requirement was extended to include the social security numbers of all children to whom support is required to be paid.

Notification to the Social Security Administration of the names of incarcerated and absconded persons. The Social Security Administration cuts off all payments to persons incarcerated in federal, state or local prison or jails, and to persons who are currently fugitives from justice. The savings to the federal budget from this provision are substantial. To implement this process, SSA needs to identify persons who have been sentenced to jail or prison and persons for whom warrants have been issued. The agency has traditionally obtained this information from state and local correctional agencies. See 42 USC § 402(x)(3) requiring Federal and State agencies to provide names and social security numbers of confined persons to the Social Security Administration. The state courts of Maryland are involved in an experimental program to provide such information directly from court records. The Maryland program has two additional future advantages for state courts. First, the program offers the possibility of obtaining better addresses for many court records; social security and other welfare agencies have the very best address records because of beneficiaries' obvious interest in maintaining their currency. Second, cutting off benefits may provide a useful incentive for persons receiving benefits to clear up outstanding warrants without requiring the expenditure of law enforcement resources to serve them.

Transmitting information to other agencies. In addition to the Social Security Administration, many states provide information from court records to other state agencies. A frequently occurring example is the Motor Vehicle Department, to which courts send records of traffic violations for enforcement of administrative driver's license revocation processes. These transfers of information often rely upon social security numbers to ensure that new citations are entered into the correct driver record.

RECENT LEGISLATION

Last year's legislation, H.R. 4857, the Social Security Number Privacy and Identity Theft Prevention Act of 2000, contained the following provision:

SEC. 102. PROHIBITION OF PUBLIC ACCESS TO SOCIAL SECURITY ACCOUNT NUMBERS POSSESSED BY GOVERNMENTAL AGENCIES

"(xi) No executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or a political subdivision thereof or trustee appointed in a case under title 11, United States Code (or person acting as an agent of such an agency or instrumentality or trustee), may display to the general public any individual's social security account number, or any derivative of such number."

This section has serious implications for state courts in a variety of contexts.

The Welfare Reform Law requires courts to enter social security numbers on court orders granting divorces or child support or determining paternity. State laws contain similar requirements in other types of cases in some states. What steps must a court take to restrict access to these documents, which are matters of public record in most states?

Social Security numbers appear in many financial documents, such as tax returns, which are required to be filed in court (e.g., for child support determinations) or are appended to official court documents, such as motions for summary judgments. What steps must a court take to restrict access to these documents, which are also matters of public record in most states?

Courts will have substantial increased labor costs in staff time to redact or strike the appearance of SSNs in paper records or in microfilm/microfiche if the above requirement is imposed.

Also, in an effort to make courts and court records more open, many courts are now beginning to make available many public records on the internet either as text/character documents or by scanning and placing them online through imaging software (PDF files). While the removal of SSN in text/character documents may be relatively easy, other scanned records, such as PDF files, will be harder to change necessitating more staff and an increase in labor costs.

COSCA RECOMMENDATIONS

We have recommended that state courts adopt the following policies, unless state law directs them otherwise:

Official court files. State courts should not attempt to expunge or redact social security numbers that appear in documents that are public records. As was mentioned earlier, federal law requires state courts to place the parties' social security numbers in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgement in order to facilitate the collection of child support. The purpose of placing that data on judgments is not just to provide it to child support enforcement agencies; it is also to provide it to the parties themselves for their own private enforcement efforts. Any other interpretation puts the courts in an untenable position—having an affirmative obligation to provide judgments in one form to parties and child support enforcement agencies and in another form to all other persons.

This same reasoning applies to income tax returns or other documents containing social security numbers filed in court. It would be unreasonable to expect courts to search every document filed for the existence of social security numbers. Further, court staff has no business altering documents filed in a case; the social security number may have evidentiary value in the case—at the very least to confirm the identity of the purported income tax filer.

Case management information databases. Data in automated information systems raises more privacy concerns than information in paper files. Automated data can be gathered quickly and in bulk, can be manipulated easily, and can be correlated easily with other personal data in electronic form. Data in an automated database can also be protected more easily from unauthorized access than data in paper files. It is feasible to restrict access to individual fields in a database altogether or to limit access to specific persons or to specific categories of persons. Consequently, state courts should take steps to restrict access to social security numbers appearing in court databases. They should not be available to public inquirers. Access to them should be restricted to court staff and to other specifically authorized persons (such as child support enforcement agencies) for whose use the information has been gathered.

Staff response to queries from the public. When court automated records include social security numbers for purposes of identifying parties, court staff should be trained not to provide those numbers to persons who inquire at the public counter or by telephone. However, staff may confirm that the party to a case is the person with a particular social security number when the inquirer already has the social security number and provides it to the court staff member.

In short, staff may not read out a social security number but may listen to a social security number and confirm that the party in the court's records is the person with that number. This is the same distinction applied to automated data base searches. This distinction is one commonly followed in federal and state courts.

GAO REPORT

Mr. Chairman, as you know, the U.S. General Accounting Office (GAO) is undertaking a study regarding the use of SSN and SSN derivatives as personal identifiers by all levels of Federal, State and local governments. The study will include recommendations regarding the most effective means of minimizing such use beyond its original purpose.

On May 11, 2001, the Board of Directors of COSCA met with analysts of the GAO regarding this study. During our meeting, we discussed the ways in which we use SSNs in our court records and the various requirements imposed upon us on the collection of SSN data as we have just outlined. We are not the only ones that GAO has interviewed to gather their information. They have also visited local government entities, such as counties, to investigate how they use SSNs in their day-to-day activities.

At minimum, Mr. Chairman, we would ask that you examine the results of this study before you consider any legislation on this issue.

Thank you for allowing us to offer our views on this important matter.

National Conference of State Legislatures
Washington, D.C. 20001
May 21, 2001

Dear Chairman Shaw:

It is with regret that I must inform you that I will be unable to testify before you and the Subcommittee on Social Security on Protecting Privacy and Preventing Misuse of Social Security Numbers. The Connecticut House of Representatives will be in session with scheduled votes throughout the day. As Deputy Minority Leader, I must be present. The National Conference of State Legislatures (NCSL) has represented the states' interest in all aspects of social security, including the issue of use of social security numbers. I currently serve on the NCSL Executive Committee Task Force on Social Security. If there are additional hearings on this important issue, I would be pleased to participate and hope that you will include me or another state legislator on behalf of the National Conference of State Legislatures (NCSL).

The National Conference of State Legislatures (NCSL) supports efforts by the federal government to protect personal identifying information, particularly efforts to protect individuals from identity theft, fraud and misuse of personal information. We applaud your efforts to address privacy protection and prevent the misuse of social security numbers. **It is critical that the states and federal government work collaboratively and cooperatively together on this issue.**

As you are well aware, state legislatures and agencies have been examining this issue and changing how we use social security numbers and how they are protected. However, NCSL must oppose efforts that would likely impose administratively burdensome and costly unfunded mandates on the states, as well as preempt state government activities. It is our hope that as we work together, responsive solutions can be crafted that will examine the costs to state and local governments as well as the transition time needed to accomplish our shared goals.

State governments, like Connecticut have examined their policies in this area and agree that the federal government should do so as well. Two years ago, I testified before the House Judiciary Committee urging Congress to rescind its 1996 mandate that states require social security numbers on the face of state driver's licenses. NCSL opposed this mandate as an unfunded mandate and preemption of state authority. States prior to passage of the act had already moved away from using social security numbers as an identifier on the Driver's License or had begun to offer individuals the option to use another number. While we were successful in eliminating this federal requirement, it illustrates that the federal government has been inconsistent in its position on the usage of social security numbers. This indecision has increased costs to state and local governments, especially costs to reprogram computers.

Before mandating changes on the state, the federal government should examine its own role in the proliferation of social security number usage. For example, Child Support Enforcement law requires states to use social security

numbers in databases, to match financial aid and employment records and, even require social security numbers on applications for state drivers licenses.

NCSL wholeheartedly agrees that government must act to protect personal identifiers, including the Social Security account number (SSN), which has come to be the primary identifier of individuals in the United States. **Yet, NCSL is concerned that without a thorough review of how various sectors of government use the SSN in day-to-day operations it will be difficult to determine how best to protect individuals from improper use of the SSN.** States have used the SSN as a unique identifier for some time, especially after some federal programs required their usage. State entities internally use SSNs in a variety of ways. SSNs are used to administer health and human services benefits for low-income families as well as employee benefits and retiree benefits. SSNs are used internally for public health programs, criminal justice systems, and state universities. SSNs are essential to tax administration and procurement systems. The costs of changing these databases to disallow the use of SSNs can be enormous.

We appreciate that you and your staff have clarified that the intent of any legislative effort on your part is to restrict display and sale of SSNs. We remain concerned however, that without a more comprehensive definition of what constitutes display, lawful and necessary use by state governments, political subdivisions and instrumentalities will be restricted. States also use SSNs as a crosscheck for fraud reduction. Due to constituent demand and recent Supreme Court decisions, states have moved to restrict and in many cases prohibit the sale of personal identifying information including the SSNs.

It is essential that federal policymakers get an accurate accounting of governmental and nongovernmental usage of social security numbers. NCSL staff has met with the U.S. Government Accounting Office (GAO) to provide information requested so that you will have the background necessary to draft comprehensive legislation that will adequately address the scope, effect and cost of the legislative changes you propose on all levels of government and on the private sector.

In Connecticut, we have examined our usage of social security numbers and made many changes to our laws and practices. This is not unusual. In many cases, state privacy statutes are stronger than protections provided under federal law. **NCSL is especially concerned about efforts to preempt state authority to ensure privacy which merely mask attempts to weaken strong state privacy statutes.** NCSL maintains that federal privacy efforts should strengthen existing protections not undermine them. Recent Connecticut privacy initiatives included:

- Repealed a requirement that municipal tax collectors collect every taxpayer's SSN. Removed a provision that was to have taken effect on December 1, 2000, requiring the Department of Motor Vehicles to give local tax assessors vehicle owners' SSNs (PA 98-261).
- Removed the SSN from the information that people who register to vote or respond to the voter canvass can voluntarily provide to registrars of voters, prohibited any voter registration official from disclosing to another government agency, as well as the public, the SSN of a voter who provided it under prior law, and removed a requirement that registrars of voters or the secretary of the state include registered voters' SSNs on the lists they must give to the jury administrator (PA 99-268).
- Made identification theft a class D felony for anyone to intentionally get another person's personal identifying information and use it for an unlawful purpose, including to get or attempt to get credit, goods, services, or medical information. The act defines "personal identifying information" as motor vehicle operator's license, Social Security Number, employee identification, demand deposit, savings account, or credit card numbers or someone's mother's maiden name (PA 99-99).
- Made sure that Registrars of Voters, and the Secretary of the State, cannot disclose SSNs to the public, nor can they use it as the voter identification number on the registry list (CGS § 9-35).
- And changed policies related to certain town officials who collect Social Security numbers (SSNs) in connection with their duties. The town clerk, as the town's registrar of vital statistics, records the SSN on marriage and death certificates, which are open records. But as a matter of practice, the clerk (1) covers the SSN when someone asks to inspect the record or (2) refers to the town's record index which shows only the names, dates, and events. The father's SSN can be included on the birth certificate of a child born out of wedlock but disclosure is restricted.

If federal law changes state government usage of SSNs, it is critical that the law defines what constitutes "use", "public display", "public access" and "derivatives of" Social Security Account Numbers. Without a clearer understanding of these con-

cepts we are concerned that implementation of the legislation will be mired with legislative, administrative and judicial pitfalls. We are very concerned about the cost and administrative impact of prohibitions on the display of SSNs and derivatives for the purposes of identification of employees. State government and its political subdivisions, agencies and instrumentalities are large employers with multiple security and related concerns that may require the use and display of SSNs by employees, including student employees at higher education institutions. Without a more thorough definition of what constitutes prohibited display; government will be left with little direction in this area. We understand that one of the intentions of the provision is to prohibit the display of the SSN on badges worn by employees for both identification and security purposes. **The costs to government to remove the SSN number from identification cards issued to employees is likely to be very high, while the bill remains silent on how these costs are to be offset.**

It is critical that we ensure adequate transition time for policy changes. We understand that a multitude of activities would be prohibited including the use of SSNs to post grades at institutions of higher learning, even when other identifying information is not provided. Given the breadth of this provision we are concerned that two years may not be sufficient time for all sectors of government to cease prohibited display. Further, we believe full implementation of this provision will be very cost prohibitive on all levels of government. We are also concerned that the cost and administrative burden associated with the removal of SSN from Commercial Driver's Licenses remains high. We suspect that state may need more time to remove SSNs from these licenses.

Additionally, it is important that the federal government pay attention to the importance of SSNs in preventing fraud. We are concerned that removal of SSNs from checks/warrants issued by government may provide increased opportunities for fraud and theft, particularly upon those who share common sur- and proper names.

Finally, states can not be liable for the actions of third party administrators or processors. States and political subdivisions should not be held liable for the actions of third party administrators and processors should these contractors engage in activities prohibited by the legislation. We would appreciate additional detail in this area.

Again, we thank you for soliciting our input on this important measure. We look forward to working with you on this legislation. Should you or your staff have questions about our concerns or require additional information, please contact Sheri Steisel, Federal Affairs Counsel and staff to our Human Services Committee or Gerri Madrid, staff to our Federal Budget and Taxation Committee at NCSL at (202) 624-5400.

Sincerely,

Representative Brian Flaherty
Deputy Minority Leader,
Connecticut House of Representatives

Statement of Bruce Hulme, National Council of Investigation and Security Services, Inc.

Good morning Mr. Chairman and members of the Committee. My name is Bruce H. Hulme and I am appearing today on behalf of the National Council of Investigation and Security Services and as Legislative Chairman of the Associated Licensed Detectives of New York State. I am a past president, chairman and currently serve as a Board member of both organizations. I have been a licensed private investigator in New York for thirty-seven years and am president of Special Investigations, Inc.

We would like to include reference to HR 2036, the Social Security Number Misuse Prevention Act of 2001, that is cosponsored by many members of this committee. As a profession that has been trying for years to help victims through the identity theft maze, we applaud the efforts of Congress to finally put laws on the books that will bring victims some relief. While a percentage of identity thieves no doubt gather their victim's identities from the Internet, our experience is that most such thefts result from the purloining of documents, files, charge slips, credit cards, and wallets from restaurants, stores, trash bins and private property. The remedies proposed by some of this legislation seem appropriate, but Congress should not expect that closing Internet information access is going to stop this crime.

Most of HR 2036 seems to be on the right track and we support Sections 102 and 301 as well as parts of Section 201 prohibiting the display of the social security

number to the general public. We believe there should be substantial criminal and monetary penalties for misuse of the social security number that causes or intends to cause harm to an individual. But we are very concerned about several Sections which, in fact, will hinder relief for victims of identity theft and many other crimes and cause unintended consequences.

A number of years ago, the Federal Trade Commission entered into a consent agreement whereby the identifying information that precedes a credit report, which is called "header" information, was deemed not part of the credit report and therefore not covered by the Fair Credit Reporting Act as a Consumer Report. The "header" report does not contain any financial information. This non-financial "header" information has been an invaluable resource for investigators to locate witnesses, heirs, debtors, and to employ in all manner of fraud and theft investigations. The language in Section 203 would codify the termination of credit header availability for any legitimate purpose beyond the controversial FTC interpretation of Gramm-Leach-Bliley. In combination with Section 201 it will make it impossible for any civilian investigator to obtain or report information necessary to identify suspects and exonerate the innocent without first obtaining the written permission of a suspect as required by the FCRA. We therefore ask that Section 201 be amended to include exemptions for business to business use such as is reflected in Section 3 of S 848 currently before the Senate Judiciary Committee. We also ask that Section 203 be amended to reflect credit header information remain available for the same purposes as reflected in Section 4 of the Drivers Privacy Protection Act.

Private investigators, for a fee, hire or reward, as a regular part of their routine, ascertain, collect, assemble, evaluate and provide their clients documents and reports containing personally identifiable information. Such information often includes the social security numbers of individuals. We also ask that Section 201 be amended to reflect that the exceptions include providers of reports prepared in connection with litigation, in anticipation of litigation, due diligence, investigation of insurance claims, civil and criminal fraud, criminal defense, identity fraud, stalking or any other violations of law. Restriction on sale and purchase of the social security number should not apply to confidential investigations of suspected crime or other legitimate business purposes. In fact, many entities such as the National Association of Security Dealers, Insurance Index Bureau and self-regulatory organizations and others that are not part of Federal or State government would be excluded from using the social security number to identify consumers for legitimate investigative purposes.

In 1997, I appeared before the Federal Trade Commission Workshop on behalf of the National Council of Investigation and Security Services to present the private investigation industry's position on consumer information privacy. That presentation helped create the record that formed the FTC's analysis of computer database services. Members of the Individual Reference Services Group testified along with others and industry practices were implemented regarding the disclosure of information that they gather and disseminate to third parties such as private investigators, insurance companies, security firms, attorneys, public interests groups and law enforcement agencies. Private investigators were found to be qualified users for permissible purposes of the data provided by IRSG member firms such as LEXIS-NEXIS, ChoicePoint-Database Technologies, Inc., Equifax, Experian and Trans Union.

There are appropriate uses for such information which are not only critical for private investigators but for attorneys, journalists, medical researchers, insurance companies, self-regulatory bodies, as well as government and law enforcement in fraud prevention, and child support enforcement. Other uses include uniting separated families, locating heirs to estates, locating pension fund beneficiaries, locating organ and bone marrow donors, significant journalistic endeavors, apprehending criminals, aiding citizens in obtaining access to public record information and in assisting the very individuals that this legislation seeks to protect.

Licensed private investigators and security service companies in my state are licensed by the New York Department of State. "The duties of a private investigator as set forth in that state's General Business Law Section 71(1) encompass various activities aimed at uncovering and/or prevention of the commission of crimes and/or torts by others, and the business of private investigation is, therefore, quasi law enforcement in nature. Licensed private investigators are, therefore, held to the highest standards of honesty, integrity and rectitude in their business dealings."

Most other states have legal jurisdiction over private investigative and security firms. They undergo fingerprint criminal background checks, are regulated, are tested and for the most part receive training and often continuing education. We believe that state regulated licensed private investigators and security firms should be allowed continued access to header information. Many of the reports that private in-

vestigators prepare which contain the social security numbers that this committee seeks to protect, are privileged attorney work product. We abhor scam and fraud doers. And we object to the rogue information brokers who advertise to the general public on the Internet that they will provide information on anybody, to anybody, for a price no matter who the customer. Publication of personally identifiable information including the social security number to the general public can only continue to lead to improper use, theft, fraud and even potential physical harm.

There are a number of bills before Congress that would ban the use of the social security number for any but its intended purpose. Many of these bills do not take into consideration the effect of removing the social security number as an identifier. We believe a good example of a viable type of solution lies in Section 3 of S 848. This legislation prohibits the wrongful use and publication of a consumer's social security number, while appearing to recognize the legitimate and necessary uses of the number. We respectfully request that section 203 of HR 2036 be amended as follows:

SEC. 203. CONFIDENTIAL TREATMENT OF CREDIT HEADER INFORMATION.

(a) IN GENERAL.—Section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a is amended by adding at the end the following new subsection:

(q) CONFIDENTIAL TREATMENT OF CREDIT HEADER INFORMATION.—Information regarding the social security account number of the consumer, or any derivative thereof, may not be furnished to any person by a consumer reporting agency other than in a full consumer report furnished in accordance with section 604 and other requirements of this title except for use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, to locate pension beneficiaries, bone marrow donors, missing persons, due diligence and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

We fully appreciate the incredible burdens faced by victims of identity theft. Many of us have had to face these victims. When all other avenues of redress have fallen upon deaf ears and often as a last resort, identity fraud victims have turned to private investigators to redeem their name and restore their good reputation. In fact, many licensed investigators have assisted these victims for little or no remuneration.

The New York State Senate Majority Task Force on the Invasion of Privacy in March 2000 made several recommendations that concern identity theft:

- Provide for an expedited process whereby identity theft victims can petition a court or administrative body to make a finding and issue an order in cases where evidence of identity theft can be clearly demonstrated, thereby facilitating efforts to restore the victim's credit history;
- Develop initiatives to curtail abusive practices of collection agencies, particularly when actions are directed at identity theft victims;
- Increase civil penalties for credit reporting agencies' willful noncompliance with the resolution of identity theft matters;
- Establish an Identity Theft/Consumer Fraud Assistance Board to provide assistance to identity theft victims and a fund for victim assistance and investigations.

The National Council of Investigation and Security Services and the Associated Licensed Detectives of New York State take the position that anyone who uses personally identifiable information or financial information for illegal purposes be subject to criminal sanctions and heavy fines. We favor the implementation of assessing enhanced penalties for aggravated cases, actual damages for willful violations, and additional damages allowed by the court for commercial purposes, disgorgement of profits, attorney's fees and costs, and additional sanctions upon the receiver of information that is obtained for unlawful purposes.

Taking away the tools from the civilian crime fighters and investigators serving the justice system is not the way to go about resolving identity theft. Congress needs to ensure that exemptions are provided for licensed private investigators on legitimate business. We would also like to see the FTC set up a liaison with our profession which would allow us to provide evidence on those who commit fraud and who tarnish our reputation.

In December 1997, the Federal Trade Commission submitted a report to Congress entitled "Individual Reference Services" wherein the list of comments submitted pursuant to Federal Register Notice comprised hundreds of letters that were received from private investigators outlining their need for continued access to credit

header records giving case-by-case examples where such information was essential. When I appeared before the FTC, I submitted hundreds of additional letters from private investigators citing examples where credit header information was the critical factor in their obtaining a successful result for their clients.

The Council believes that licensed private investigators, and for that matter licensed security firms, should continue to be allowed access to credit header information. The Drivers Privacy Protection Act of 1994, enacted after Congressional hearings during which the Council testified, permitted a licensed private investigative agency or licensed security service access to personally identifiable information for lawful purposes. As stated earlier, we would like this committee to consider similar provisions in the present legislation being discussed today.

We have recently surveyed our membership about how they have been able to assist victims of identity theft. The following examples demonstrate some of the benefits of permitting licensed private investigators to access essential information from "credit headers." Section 203 of HR 2036 would deny us this critical tool. These anecdotes should give this Committee some idea of the types of cases that require this information:

In New York, a public utility hired our member to conduct a pre-employment background investigation for a high level position. A credit report, obtained under the FCRA contained two different social security numbers. Running a credit header check on the second number revealed a different name and addresses and the investigator discovered his true identity. The applicant had adopted the identity of one of his former college professors to keep his own less desirable background secret.

In Atlanta, Georgia, an auto dealership asked our investigator to help an applicant who claimed his identity had been stolen. An imposter had stolen this man's social security number and date of birth as well as the identity of four other people. His criminal record included nine felonies in Georgia and other multi-state offenses. The applicant couldn't understand why he had been turned down for several jobs until one potential employer leveled with him and he realized his identity had been stolen. Numerous law enforcement agencies told him they couldn't help him. Our investigator arranged for the applicant to be fingerprinted and the Georgia Bureau of Investigation issued him a certificate stating he was not the same person as the imposter. He then carried the certificate to the three major credit bureaus to clear his name in their files. The investigator says had he not helped the victim through this maze, he would surely have been arrested in Georgia or Florida where warrants had been issued.

In San Francisco, an investigator reports working a case for a successful business owner who started getting statements in the mail saying he owed tens of thousands of dollars on computers and other purchases, none of which he knew anything about. He found someone had hijacked his identity, opened credit card and store accounts in his name and had even opened a web page mirroring his web page and had an email address similar to his. The San Francisco Police said they would take a report, but would not investigate and suggested he go to the Secret Service. The Secret Service said they would not handle the case until at least $100,000 is lost. Current losses are approaching $80,000. The victim had a suspicion it was an ex-employee who lived in Salt Lake City and called the investigator. The agency used credit header information to learn that the ex-employee has three names, three or four social security numbers, and three different dates of birth on file. The investigators still don't know if he is involved, but they continue looking for linkages. They also located an address to which computers were shipped and are currently running down as much information as they can on the owners and occupants of that address.

As we said before, licensed private investigators are an important integral part of the civil and criminal justice systems. The job of the criminal defense investigator is to gather evidence to assure a fair trial for persons rightly or wrongly accused of crime. One of the primary and most cost-effective tools available to locate witnesses is the credit header. As a matter of fairness, even ex-law enforcement members admit that restricting access to credit headers will tip the scales in favor of law enforcement and augurs against the defendant's ability to receive a fair trial. Law enforcement agencies have NCIC and many other means at their disposal, and are always exempted from legislation restricting access to the same information sources that HR 2036 would deny licensed private investigators. But after July 1, 2001, the criminal defendant's investigator will have no such tools and usually very little money to spend on locating key witnesses.

At a time when our justice system is being criticized for errors proven by DNA evidence, we find it hard to believe that Congress intended to take away a defendant's primary means of locating witnesses. Yet that is exactly what the FTC inter-

pretation of Gramm-Leach-Bliley has done. And the present language of HR 2036 would codify the FTC interpretation.

We believe that the identity theft laws recently enacted will help law enforcement to prosecute perpetrators once apprehended. But Congress should be aware that public law enforcement resources are stretched and crimes of this nature are still not a high priority. The losses, though devastating to the victims, are usually beneath the dollar threshold that many departments follow. And the mental toll on the victims is unquantifiable. The private sector will have to continue to augment public law enforcement. And it should be noted that the hapless victims of this crime often have very limited resources.

To the extent HR 2036 will prohibit rogue information brokers from displaying and selling the social security number and deter identity theft, we commend it. But Congress should proceed very carefully before eliminating the very tools used to apprehend the stealers of the identities of others or the perpetrators of other criminal acts.

Thank you for the opportunity to address these important issues.

Statement of Cynthia L. Moore, National Council on Teacher Retirement, Arlington, Virginia

I appreciate the opportunity to submit a statement for the record in connection with the hearing on protecting privacy and preventing the misuse of Social Security numbers. I will confine my comments to the uses of Social Security numbers by state and local government retirement systems as they carry out a critical personnel function for states and localities: the efficient administration and sound funding of the retirement programs that serve state and local government employees. I encourage the Subcommittee members to consider these comments as they debate H.R. 2036, the Social Security Privacy and Identity Theft Prevention Act of 2001, sponsored by Chairman Shaw.

The National Council on Teacher Retirement is made up of 75 state and local government retirement systems that include teachers and other public employees. Together, the retirement systems serve over 11,000,000 state and local government employees. They hold assets in excess of $2 trillion to pay pension, disability, and other benefits to employees and their beneficiaries. Assets not needed to pay immediate benefits are invested to produce earnings. These earnings reduce the amount of funding that both individual employees and taxpayers must pay to support the benefits.

State and local government retirement systems feel strongly that individuals must be protected from the fraudulent and other wrongful use of their Social Security numbers. The means to reach that goal requires a delicate balance, however. As I will describe in this statement, the retirement systems use Social Security numbers to assist them in performing the role of administering retirement and other benefits and we ask that these uses be preserved.

State and local government retirement systems use Social Security numbers in many ways. I will provide some examples.

Transactions between Retirement System and Plan Participant

- As the primary retirement account number for a plan participant;
- As a means to match a specific individual with a corresponding benefit;
- As an identifier on checks, annual statements, and correspondence;
- As a tracking number for participant records;
- As an identifier for health insurance benefits;
- As a means to ensure that death benefits are paid to the participant's intended beneficiary;
- As an identifier for federal tax reporting purposes; and
- As a means to ensure the identity of a particular participant in the case of several participants with identical names.

Transactions between Retirement System and Plan Participant's Employer

The uses listed above ensure that an individual receives the benefits to which he/she is entitled. Equally important are the uses of Social Security numbers involving the plan participant's employer. In the case of a teacher retirement system, the employer of an individual teacher is the school district. It must provide the retirement system with information about the teacher's years of service credit and salary. The school district may also remit contributions it makes on behalf of the teacher. Social

Security numbers are used to "tag" information and contributions to the applicable teacher. Such use ensures that the information is properly reported and correct amounts of contributions are received. Without such identification, inaccurate data about service credit and salary might be provided to the retirement system. Moreover, if inadequate contributions are made, the retirement system will not have the funds sufficient to pay promised benefits. Conversely, if excess contributions are mistakenly made, taxpayers have paid more than necessary to support the retirement program.

Transactions to Uncover Fraudulent Use of Retirement System Benefits

A retirement system's paramount purpose is to act for the exclusive benefit of the plan participants. To carry out this aim, the system safeguards the funds available to pay benefits, not only as they come into the system, but also as they are paid out. A common way to verify that benefits are correctly paid is through comparison of retirement system records with Social Security data. For example, a system matches plan participants, using Social Security numbers, against the Social Security Administration's list of deceased persons. If any match is revealed, the retirement system may be unknowingly paying a benefit that is being cashed, in the case of a check, or withdrawn, in the case of a direct deposit, by an unauthorized individual. By using Social Security numbers, the system can stop any fraudulent receipt of benefits thereby ensuring that adequate funding is available to pay lawful benefits.

The foregoing uses relate to the essential personnel functions of state and local governments. They ensure that participants receive the benefits to which they are entitled. They verify that employers are paying the correct amount of contributions and sharing the information needed to ensure timely and accurate payment of benefits. Moreover, uncovering fraudulent activity protects the funds in the retirement system and preserves them to be used for lawful purposes. None of these uses address the problems that H.R. 2036 seeks to remedy, such as the sale of Social Security numbers and the public display of them. Mr. Chairman, I respectfully ask you and the members of the Subcommittee to recognize and preserve these uses of Social Security numbers by the retirement systems. The uses are legitimate ways to achieve the efficient administration and sound funding of the retirement programs that serve state and local government employees.

Thank you again for the opportunity to provide comments on this important issue. Should you or your staff have any questions, please contact me at 703-243-1667.

Statement of the Hon. Ron Paul, a Representative in Congress from the State of Texas

I wish to thank the subcommittee on Social Security of the Ways and Means Committee for holding this hearing on the misuse of the Social Security number. The transformation of the Social Security number into a de facto uniform identifier is a subject of increasing concern to the American people. This is, in large part, because the use of the Social Security number as a standard identifier facilitates the crime of identity theft. Today, all an unscrupulous person needs to do is obtain someone's Social Security number in order to access that person's bank accounts, credit cards, and other financial assets. Many Americans have lost their life savings and have had their credit destroyed as a result of identity theft.

The responsibility for the misuse of the Social Security number and the corresponding vulnerability of the American people to identity crimes lies squarely with the Congress. Since the creation of the Social Security number, Congress has authorized over 40 uses of the Social Security number. Thanks to Congress, today no American can get a job, open a bank account, get a professional license, or even get a drivers' license without presenting their Social Security number. So widespread has the use of the Social Security number become that a member of my staff had to produce a Social Security number in order to get a fishing license!

Because it was Congress which transformed the Social Security number into a national identifier, Congress has a moral responsibility to address this problem. In order to protect the American people from government-mandated uniform identifiers which facilitate identity crimes, I have introduced the Identity Theft Prevention Act (HR 220). The major provision of the Identity Theft Prevention Act halts the practice of using the Social Security number as an identifier by requiring the Social Security Administration to issue all Americans new Social Security numbers within five years after the enactment of the bill. These new numbers will be the sole legal

property of the recipient and the Social Security Administration shall be forbidden to divulge the numbers for any purposes not related to the Social Security program. Social Security numbers issued before implementation of this bill shall no longer be considered valid federal identifiers. Of course, the Social Security Administration shall be able to use an individual's original Social Security number to ensure efficient transition of the Social Security system.

This act also forbids the federal government from creating national ID cards or establishing any identifiers for the purpose of investigating, monitoring, overseeing, or regulating private transactions between American citizens, as well as repealing those sections of the Health Insurance Portability and Accountability Act of 1996 that require the Department of Health and Human Services to establish a uniform standard health identifier. By putting an end to government-mandated uniform IDs, the Identity Theft Prevention Act will prevent millions of Americans from having their liberty, property and privacy violated by private-and-public sector criminals.

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

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

Other members of Congress will claim that the federal government needs the power to monitor Americans in order to allow the government to operate more efficiently. I would remind my colleagues that in a constitutional republic the people are never asked to sacrifice their liberties to make the job of government officials a little bit easier. We are here to protect the freedom of the American people, not to make privacy invasion more efficient.

Mr. Chairman, while I do not question the sincerity of those members who suggest that Congress can ensure citizens' rights are protected through legislation restricting access to personal information, the only effective privacy protection is to forbid the federal government from mandating national identifiers. Legislative "privacy protections" are inadequate to protect the liberty of Americans for several reasons. First, it is simply common sense that repealing those federal laws that promote identity theft is more effective in protecting the public than expanding the power of the federal police force. Federal punishment of identity thieves provides old comfort to those who have suffered financial losses and the destruction of their good reputation as a result of identity theft.

Federal laws are not only ineffective in stopping private criminals, they have not even stopped unscrupulous government officials from accessing personal information. Did laws purporting to restrict the use of personal information stop the well-publicized violation of privacy by IRS officials or the FBI abuses by the Clinton and Nixon administrations?

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

Mr. Chairman, those members who are unpersuaded by the moral and constitutional reasons for embracing the Identity Theft Prevention Act should consider the overwhelming opposition of the American people toward national identifiers. The overwhelming public opposition to the various "Know-Your-Customer" schemes, the attempt to turn drivers' licenses into National ID cards, HHS's misnamed "medical privacy" proposal, as well as the numerous complaints over the ever-growing uses of the Social Security number show that American people want Congress to stop invading their privacy. Congress risks provoking a voter backlash if we fail to halt the growth of the surveillance state.

In conclusion, Mr. Chairman, I once again thank you and the other members of the subcommittee for holding a hearing on this important issue. I hope this hearing would lead to serious Congressional action to end to the federal government's unconstitutional use of national identifiers which facilitate identity theft by passing HR 220, the Identify Theft Prevention Act.

○