epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Protecting the Privacy of the Social Security Number from Identity Theft"

Before the

Subcommittee on Social Security.
Committee on Ways and Means
United States House of Representatives

June 21, 2007
B-318 Rayburn House Office Building
Washington, DC

I. Introduction

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, thank you for the opportunity to testify on the misuse of the Social Security Number and the escalating problem of identity theft

My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C.[1] Founded in 1994, EPIC has participated in the leading cases involving the privacy of the Social Security Number and has frequently testified in Congress about the need to establish privacy safeguards for the Social Security Number to prevent the misuse of personal information.[2]

Two weeks ago in testimony, I urged the Subcommittee to strengthen the privacy safeguards for the proposed Employment Eligibility Verification Systems and warned that the errors in the Basic Pilot will be exacerbated by the increased dependence on the SSN.[3] And, about a year ago, I urged Members of this Subcommittee to reject the use of the SSN as a national identifier and to ensure the development of adequate privacy and security safeguards to address the growing crisis of identity theft.[4]

Today, my statement will focus on the dramatic increase in identity theft in the United States that has resulted directly from the misuse of SSN and the need to pass comprehensive legislation to limit the use of the SSN as well the need to develop better systems of identification that are more robust.

II. Summary of Social Security Number History

Social Security numbers have become a classic example of "mission creep," where a program designed for a specific, limited purpose has been transformed for additional,

---

[1] EPIC maintains an archive of information about the SSN online at http://www.epic.org/privacy/ssn/ ["EPIC SSN Page"].

[2] *See, e.g.*, *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) ("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"); Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Chris Jay Hoofnagle, Legislative Counsel, *EPIC, Testimony at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the H. Ways & Means Subcom. on Social Security & the H. Judiciary Subcom. on Immigration, Border Sec. & Claims,* 105th Cong. (Sept. 19, 2002), *available a*t http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[3] Marc Rotenberg, President, EPIC, *Testimony at a Hearing on Employment Eligibility Verification Systems Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (June 7, 2007), *available at* http://www.epic.org/privacy/ssn/eevs_test_060707.pdf.

[4] Marc Rotenberg, President, EPIC, *Testimony at a Hearing on Social Security Number High-Risk Issues Before the H. Ways & Means Subcom. on Social Security,* 109th Cong. (Mar. 16, 2006), *available at* http://www.epic.org/privacy/ssn/mar_16test.pdf.

unintended purposes, some times with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security.

These risks associated with the expanded use of the Social Security Number and identification cards underscore the importance of the hearing today.

The SSN was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers' contributions to the Social Security fund. Legislators and the public were immediately distrustful of such a tracking system, which can be used to index a vast amount of personal information and track the behavior of citizens. Public concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

Over time, however, legislation allowed the SSN 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.

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 we face today. Although the term "identify 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."[5]

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and included provisions to limit the uses of the SSN. The Privacy Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose his or her 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."[6] The Privacy Act makes clear Congress' recognition of the dangers of widespread use of SSNs as universal identifiers.

The Senate Committee report stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of

[5] Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125-35 (MIT 1973), *available at* http://www.epic.org/privacy/hew1973report/.
[6] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).

privacy concerns in the Nation." Short of prohibiting the use of the SSN outright, Section 7 of the Privacy Act provides that any agency requesting that an individual 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." This provision 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 that 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.

But the reality is that today the SSN is the key to some of our most sensitive and personal information. The financial services sector, for instance, has created a system of files, keyed to individuals' SSNs, containing personal and financial information on nearly 90 percent of the American adult population. This information is sold and traded freely, with virtually no legal limitations. In addition, credit grantors rely upon the SSN to authenticate a credit applicant's identity. Many cases of identity theft occur when thieves apply using a stolen SSN and their own name. Despite the fact that the names, addresses, or telephone numbers of the thief and victim do not match, accounts are opened and credit granted using only the SSN as a means of authentication.[7]

Even the government is susceptible to identity theft based solely on obtaining an SSN and the name associated with it. Stolen SSNs are used to file fraudulent tax returns and to seek refunds owed to other citizens. When the proper owner of the SSN files his tax return it may be rejected as a duplicate and he may be required to spend time fixing his records in order to receive his tax refund.[8]

III. President's ID Theft Task Force and Nexus Between SSNs and Identity Theft

The growing misuse of the Social Security Number and the associated problem of Identity Theft have not escaped the notice of the White House. In May 2006, the President established an Identity Theft Task Force to "track down on the criminals who traffic in stolen identities and protect American families from this devastating crime."[9] The Task Force, chaired by the Attorney General and the FTC Chair, was expected to protect the financial information of citizens and reduce the threat of identity theft, which the FTC now annually reports is the number one concern of American consumers.[10]

---

[7] *See, e.g.*, *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (Credit reporting agencies issued credit reports to identity thief based on SSN match despite address, birth date, and name discrepancies); *Dimezza v. First USA Bank, Inc.*, 103 F. Supp.2d 1296 (D. N.M. 2000) (same). *See also United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003) (Credit issued based solely on SSN and name, despite clear location discrepancies); *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997) (same); *Vazquez-Garcia v. Trans Union De P.R., Inc.*, 222 F. Supp.2d 150 (D. P.R. 2002) (same).

[8] President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 21 (April 23, 2007) ["ID Theft Task Force Report"], *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[9] Press Release, Office of the Press Sec'y, Fact Sheet: The President's Identity Theft Task Force (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html.

[10] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

EPIC participated in the task force proceedings and provided extensive comments.[11] We supported the Task Force's recommendation to reduce reliance on SSNs at all levels of government. We said:

> Reducing use of SSNs and limiting the amount of data collected by government bodies is fundamental to maintaining the security of consumer data. This is an especially critical limitation upon the public sector, since government has the power to compel individuals to disclose personally identifiable information. The personal data collected by government entities should never be disseminated in public records or sold to the private sector. The Task Force should curtail the publicly available sources of the SSN, including the Social Security Death Register; bankruptcy filings and other court records; birth and death records; and records of other life events.[12]

EPIC also pointed to the growing problem of the misuse of the SSN by businesses:

> The Task Force should also carefully investigate and analyze SSN use in the private sector, as there is evidence that private sector use of SSNs contributes substantially to the problem of identity theft. Restricting the sale, purchase and display of SSNs by private entities is a critical consideration in combating identity theft. The private sector must move away from using SSNs as identifiers, a goal which is feasible as demonstrated by Empire Blue Cross' transition from SSNs to alternative identification numbers for its 4.8 million customers.[13]

The President's Task Force recognized the connection between the misuse of the Social Security Number and the crime of identity theft but failed to propose adequate safeguards. According to the President's Identity Theft Task Force, "the SSN is especially valuable to identity thieves, because often it is the key piece of information used in authenticating the identities of consumers."[14] The SSN is also commonly used by the government and entities in the private sector to identify individuals. As the Task Force noted, "SSNs … are widely used in our current marketplace to match consumers with their records (including their credit files) and as part of the authentication process."[15] In short, SSNs function as both a username and a password – a single piece of information that both identifies an individual and authenticates that identification, a lock and a key rolled into one. Because of the way in which the SSN is used for identification and the prevalence of that use, much of your most sensitive information does not even have the same sort of rudimentary security as your email account.

---

[11] EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.
[12] *Id*. at 8.
[13] *Id*. at 8-9.
[14] ID Theft Task Force Report at 23, *supra* note 8.
[15] *Id.* at 44.

As noted by the Task Force, "the SSN is a critical piece of information for the thief, and its wide availability increases the risk of identity theft."[16] Despite the problems associated with using the SSN as an identifier, the federal government routinely uses SSNs in order to identify individuals within governmental programs. SSNs have been included as part of Medicare's Health Insurance Claim Number,[17] and as part of a federal award identifier used by the USDA.[18]

IV. Identity Theft as a Result of Social Security Number Misuse

During the past fiscal year, the Department of Justice charged 507 defendants with aggravated identity theft. The DOJ highlighted a number of these prosecutions in a recent press release.[19] A handful of the cases the DOJ put on display involved defendants misusing Social Security numbers for illegal purposes.

In one of the cases, a woman was sentenced to 75 months imprisonment for defrauding FEMA in the wake of Hurricane Katrina.[20] The defendant filed 28 fraudulent claims for disaster relief to FEMA using other people's Social Security numbers. After receiving money from FEMA, the defendant went out to buy real estate, a mobile home, vehicles, electronics, furnishings, and other goods and services.

In another case, six defendants victimized AOL subscribers with a "phishing" scheme.[21] The defendants "spammed" thousands of AOL users with emails containing fake electronic greeting cards. When the subscribers tried to open the friendly greeting, they were instead met with a software trojan that prevented the users from accessing AOL without entering sensitive information including bank account, address, and Social Security numbers. The defendants used the stolen information to make counterfeit debit cards, which they swiped at ATM machines to get cash, and used at online and retail stores to buy goods and services. It appears that we've gone from "Hello, you've got mail!" to "Hello, you got your identity stolen!"

Another defendant was paid to fraudulently use Social Security numbers and other confidential info to get personal phone records of reporters and Hewlett-Packard officials, as well as their family members.[22] This case is a clear example of "pretexting" or posing as somebody else to obtain sensitive calling records. And these are just the cases the DOJ chose to highlight.

---

[16] *Id*. at 42.
[17] *Id*.
[18] Ellen Nakashima, *U.S. Exposed Personal Data: Census Bureau Posted 63,000 Social Security Numbers Online*, WASH. POST, Apr. 21, 2007, at A05, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/04/20/AR2007042002208.html.
[19] Press Release, Dep't of Justice, Fact Sheet: The Department of Justice's Efforts to Combat Identity Theft (Apr. 23, 2007), *available at* http://www.usdoj.gov/opa/pr/2007/April/07_opa_278.html.
[20] *Id*.
[21] *Id*.
[22] *Id*.

There's also the case of 19 year-old Irving Escobar who bought stacks of $400 gift cards from Wal-Mart and cashed them in to buy electronics.[23] Escobar went on lavish shopping sprees, charging as much as $112,000 in goods at gift stores. Escobar purchased, in total, an estimated $1 million in goods. Amy Osteryoung, assistant statewide prosecutor who handled the case for Florida Attorney General Bill McCollum referred to Escobar's actions as "[m]odern day money laundering."[24] Also, "Investigators believe it is the boldest tangible evidence of criminals cashing in on hacked data from TJX — the nation's largest reported computer data breach, which TJX disclosed in January."[25] TJX says it will pay for a credit-monitoring service to help avert identity theft for customers whose driver's license numbers were the same as their Social Security numbers and were believed stolen. For others, the damage has already been done.

V. Recent Social Security Number Breaches in the Federal Government

The Social Security Administration's Office of Inspector General said that 16 percent of the 99,000 fraud cases it investigated in the one-year period ending Sept. 30, 2006 involved the misuse of Social Security numbers.[26] Considering the following cases of breaches in Social Security number data storage, that number might be on the rise.

Recently, a woman named Marsha Bergmeier was bored and did an Internet search for her farm's name in Illinois.[27] She discovered a link to fedspending.org, a Web site created by OMB Watch to monitor federal spending. While clicking around the site, a searchable database popped up for her, containing information about her farm loan amount under an Agriculture Department program. Not only that, she also discovered the list of 28,000 SSNs, including her own. Published right there for everybody with an Internet connection to see.[28] The site had been up since 1996. And that's just the United States Department of Agriculture.

The Department of Defense uses Social Security numbers for just about everything[29]; from troop rosters to the dog tags dangling from soldiers' necks. Since 2006, data about almost 30 million active and retired service members has been stolen from four Veterans Affairs offices. That's approximately 30 percent of the 100 million total reported lost or stolen personal data in the United States.[30] That's a lot.

---

[23] Jon Swartz and Byron Acohido, *TJX data theft leads to money-laundering scam*, USA TODAY, June 12, 2007, *available at* http://www.usatoday.com/money/2007-06-11-tjx-data-theft_N.htm.
[24] *Id*.
[25] *Id*.
[26] *Id*.
[27] Ellen Nakashima, *U.S. Exposed Personal Data: Census Bureau Posted 63,000 Social Security Numbers Online*, *supra* note 18.
[28] *Id*.
[29] Byron Acohido and Jon Swartz, *Military personnel prime targets for ID theft*, USA TODAY, June 15, 2007, *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts_N.htm?csp=34.
[30] *Id*.

And that's a lot more than an active military service member needs to be dealing with. With increasing frequency, scam artists are setting their sights on military personnel. As USA Today reported, Marine Corporal Jacob Dissmore, 22, returned from Iraq in 2006 to learn that someone in San Diego had opened a credit card account, started a T-Shirt business and even purchased a house with Dissmore's money using his personal information.[31]

A retired Navy chief petty officer that keeps meticulous financial records suspects the theft of laptops from the Veterans Affairs office is directly responsible for suspicious activity on his accounts.[32] Earl Laurie Jr. takes care of his private info very well; he uses a P.O. Box, shreds his papers, and avoids online banking. Mr. Laurie never had a problem until right after the laptop was stolen when he started getting phone calls asking him to confirm strange credit card applications on his account.

And the American Red Cross has even had to issue warnings to military families. Identity thieves have stooped to the lowest level. The families of active military officers have reportedly been receiving phone calls from scammers pretending to be with the Red Cross delivering unfortunate news about a soldier stationed in Iraq.[33] The scammers tell the families that their loved one is being airlifted to a hospital in Germany and will not receive medical treatment unless they offer up personal information immediately. One moment you'll think the Red Cross is helping you out, the next thing you know you're a victim.

It doesn't stop there. Residents in every state of every member of this Subcommittee have experienced massive data breaches in the past year.[34]

- In Michigan, Congressman Levin, the details of a scientific study were lost on a small flash drive at the Michigan Department of Community Health in Detroit. The small flash drive contained the personal information and SSNs of 4,000 Michigan residents.[35]

- The Medicare drug benefit applications of 268 residents from Minnesota and North Dakota were recently stolen from an insurance agent's unlocked car. The applications contained applicants' name, address, date of birth, SSN, and bank routing information.[36]

---

[31] *Id*.
[32] *Id*.
[33] Jerry Carnes, *Scammers Target Soldiers' Families,* 11 ALIVE NEWS*,* May 30, 2007*, available at* http://www.11alive.com/news/article_news.aspx?storyid=97757.
[34] Privacy Rights Clearinghouse, *A Chronology of Breaches*, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[35] *Id*.
[36] *Id*.

- The Pennsylvania Department of Transportation's driver's license facility in Dunmore had computer equipment containing the Social Security of over 11,000 drivers. Also stolen were supplies used to create driver's licenses and photo IDs.[37]

- In February of last year, Congressman Davis, a computer was stolen at the University of Alabama-Birmingham, containing nearly 10,000 Social Security numbers and the personal information of potential kidney donors and recipients.[38]

- In California, it is difficult to figure out which data breach to highlight--- there were just too many to pick just one. Last year, hackers gained access to a UCLA database containing the Social Security numbers and personal information for over 800,000 current and former students, applicants, parents, and staff members. 800,000.[39]

- And Texas. Everything is bigger in Texas, even the data breaches. Texas Guaranteed Student Loan Corp. announced last year that a total of 1.7 million people's information had been compromised.[40]

- Congresswoman Tubbs Jones, Ohio was in the news just last week when an intern's car was broken into, and somebody made off with the Social Security numbers of approximately 75,000 state employees.[41]

- State employees in Kentucky received mail last year from Kentucky Personnel Cabinet. The mail had their Social Security numbers visible from the see-through plastic windows in the envelope.[42]

- And, Congressman Ryan, documents containing the personal information of Wisconsin's state assembly members were recently stolen from a legislative employee's car while she exercised at a local gym.[43]

Social Security numbers are being stolen in every state in this country.

VI. Solutions to the use of SSNs in Identity Theft

Although the Presidential Task Force on Identity Theft correctly identified many of the problems associated with SSN usage and identify theft, it failed to propose many of the obvious solutions. The Task Force noted that, as long as SSNs continue to be used as forms of authentication, thieves must be prevented from obtaining them, but it did not come up with any substantive improvement that could bring about that end.[44]

---

[37] *Id*.
[38] *Id*.
[39] Privacy Rights Clearinghouse, *A Chronology of Breaches*, *supra* note 35.
[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] ID Theft Task Force Report at 23, *supra* note 8.

The Task Force did note that unnecessary usage of SSNs in the public sector must be decreased[45] and suggested that the "[Office of Personnel Management] should take steps to eliminate, restrict, or conceal the use of SSNs (including assigning employee identification numbers where practicable), in calendar year 2007."[46] Furthermore the Task Force suggested that "[i]f necessary to implement this recommendation, Executive Order 9397, effective November 23, 1943, which requires federal agencies to use SSNs in 'any system of permanent account numbers pertaining to individuals,' should be partially rescinded."[47] Unfortunately, however, the Task Force did not propose that the SSN stop being used for purposes beyond its original intent. Instead, the Task Force conceded that "[t]he use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, however, is expressly authorized by statute and should continue to be permitted."[48]

Although the Task Force recommended that the Office of Personnel Management take a leading role in issuing policy guidance on appropriate use of SSNs[49] and create a list of acceptable SSN practices in order to determine best practices,[50] the Task Force did not lay out any basic framework for this policy guidance or any suggested best practices. Furthermore, although the Task Force suggested that a comprehensive record on the private sector use of SSNs should be developed,[51] it failed to detail how the information comprising this record ought to be recorded or what legislative changes would be necessary to reduce the crime of identity theft. The absence of a legislative recommendation on this key point is significant; in many other areas of the report, the Department of Justice recommend legislative changes to expand its own investigative and prosecutorial authority.

The task force recognizes the dangers of Social Security numbers' dual role in identification and authentication, but it fails to recommend that the Social Security number's role in authenticating an identity be completely eliminated and its use in the private sector limited. Although the Task Force adequately highlights some of the problems associated with SSN usage, it fails to provide a meaningful starting point for the government to act to correct the problems and it does not recommend, as it ought to, that the private sector immediately cease use of SSN for authentication purposes.

What else should be done?

- For starters, an effective law would limit the collection and the use of the SSN. It would be far preferable to reduce the crime of identity theft at its source than to create new enforcement authority for a problem that is clearly out of control.

---

[45] *Id.* at 24.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] ID Theft Task Force Report at 26, *supra* note 8.
[50] *Id.*
[51] *Id.*

- The use of the SSN should be limited to those circumstances that are 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.

- 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.

- 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.

- 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 the "867-00-0909" where there is no intent to commit fraud. (The number displayed could not be an actual SSN.)

- Encourage the continued development of alternative, less intrusive means of identification. We believe that the National Research Council should be funded to undertake further research on new techniques that enable records management while minimizing privacy risks.[52]

It is also important not to preempt innovative state laws that reduce the risk of SSN misuse. Many states have enacted legislative protections for the SSN. They vary from comprehensive frameworks of protection for the SSN to highly-specific laws that shield the SSN from disclosure in specific contexts.

For example, a 2005 Arizona law prohibits the disclosure of the SSN to the general public, the printing of the identifier on government and private-sector identification cards, and establishes technical protection requirements for online transmission of SSNs.[53] The law also prohibits printing the SSN on materials mailed to residents of Arizona. Exceptions to protections are limited–companies that wish to continue to use the SSN must do so continuously, must disclose the use of the SSN annually to consumers, and must afford consumers a right to opt-out of continued employment of the SSN.

A 2004 Ohio law limits the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state.[54] The law requires the establishment of policies for safe destruction of documents containing the SSN. Insurance companies

---

[52] *See also* Nat'l Research Council, WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY (Stephen Kent & Lynette Millett eds. 2003); Nat'l Research Council, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE (James Waldo, Herbert S. Lin & Lynette Millett eds. 2007).
[53] Ariz. Rev. Stat. § 44-1373.
[54] *Available at* http://www.state.co.us/gov_dir/leg_dir/olls/sl2004a/sl_393.htm.

operating in the state must remove the SSN from consumers' identification cards. Finally, the legislation creates penalties for individuals who use others' personal information to injure or defraud another person.

In Georgia, businesses are now required to safely dispose of records that contain personal identifiers.[55] The Georgia law requires that business records — including data stored on computer hard drives — must be shredded or in the case of electronic records, completely wiped clean where they contain SSNs, driver's license numbers, dates of birth, medical information, account balances, or credit limit information. The Georgia law carries penalties up to $10,000.

In the past year, Illinois has passed several laws to protect consumer privacy, including measures that address identity theft, limit the use of the Social Security Number, require notification of security breaches, and allow state residents to put a security freeze on their credit report if they believe their personal information has been compromised.[56]

Six state legislatures, in the past two months, have passed laws going against a new federal ID requirement.[57] The law would require 240 million Americans to get new licenses by 2013. The new identification cards would contain residents SSN, home address, and that they are in the USA legally. Implementation of this new ID program would cost states more than $11 billion[58], according to the National Conference of State Legislatures. The federal government has estimated that REAL ID will cost $23.1 billion.[59] Some state lawmakers have gone as far to call this federal effort an attempt to create a "'papers-please' society."[60] Without all 50 states complying, it's not really a National ID card. In the end states will have their way.

The innovative solutions that state legislatures are developing to address privacy concerns should be encouraged. The states are laboratories of democracy, and are moving effectively on emerging issues. A federal privacy baseline ensures safeguards in those states where they do not currently exist, and leaves states free to develop better protection. Even a sensible national law will become outdated as technology and business practices evolve.

---

[55] *Available at* http://www.epic.org/privacy/ssn/sb475.html.
[56] Press Release, Office of the Governor, Governor Blagojevich calls on Veterans Administration to provide immediate protection to veterans whose personal information was stolen (May 24, 2006), *available at* http://www.illinois.gov/PressReleases/ShowPressRelease.cfm?RecNum=4920&SubjectID=26
[57] Thomas Frank, *6 States defy law requiring ID cards*, USA TODAY, June 18, 2007, *available at* http://www.usatoday.com/news/nation/2007-06-18-id-cards_N.htm?loc=interstitialskip.
[58] Id.
[59] Dep't of Homeland Sec., Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10,819, 10,845 (Mar. 9, 2007), available at http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm; see generally, EPIC, Page on National ID Cards and the REAL ID Act, http://www.epic.org/privacy/id_cards/.
[60] Thomas Frank, 6 States defy law requiring ID cards, supra note 57.

EPIC also favors technological innovation that enables the development of context-dependent identifiers. Such a decentralized approach to identification is consistent with our commonsense understanding of identification. If you're going to do banking, you should have a bank account number. If you're going to the library, you should have a library card number. If you're renting videos from a video rental store, you should have a video rental store card number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.

We believe that this is also the approach favored by businesses and cutting-edge technology firms that think carefully about the issue, though it has taken us some work to make this clear. EPIC filed a complaint with the Federal Trade Commission in 2001 about Microsoft Passport, an identity scheme proposed for the Internet.[61] Microsoft was signing up users for a service that produced a single username and password for all of their Web services, including credit card information and a vast user profile. Microsoft Passport stored user information in a central database. The problem was that while Microsoft Passport claimed to enhance security, it actually had a lot of holes. And, if you accidentally left your user profile up on a public computer terminal or a malicious hacker gained access to one of your accounts, they would have access to everything associated with your user profile.

We urged the Federal Trade Commission to investigate, and the FTC eventually agreed with EPIC's position.[62] Microsoft backed off Passport, developed an approach to identity management that allowed for multiple forms of online identification, and other companies, including open source developers, followed a similar approach. [63]

I believe there is now consensus in the online community about the need to avoid single identifiers and to promote multiple identification schemes, and that this approach is best not only for privacy but also for security. The critical question is whether Congress can make physical identity systems similarly robust.

VII. The Social Security Number Protection Act, H.R. 948

H.R. 948, the Social Security Number Protection Act of 2007, has passed before the Committee on Energy and Commerce and has been reported to the House. The purpose of H.R. 948 is to prohibit the display and purchase of Social Security numbers in interstate commerce pursuant to rules to be promulgated subsequent to the passage of the

[61] EPIC maintains an archive of information about Microsoft Passport at http://www.epic.org/privacy/consumer/microsoft/passport.html.
[62] Fed. Trade Comm'n, *Agreement*, *In Re Microsoft*, FTC Docket No. C-4069 (Dec. 20, 2002).
[63] Kim Cameron, *The Laws of Identity*, Identity Weblog, Dec. 9, 2004, http://www.identityblog.com/stories/2004/12/09/thelaws.html; Windows CardSPace, http://cardspace.netfx3.com/; OpenCard, http://www.opencard.org/.

bill. Although we generally favor the bill, we believe it can be strengthened in several key areas. Most critically, there should be clear guidance to the FTC to limit the sale and purchase of Social Security numbers, there should be private right of action for individual citizens to ensure that the law is effective, and there should be no preemption of state law.

Sections 3(a)(1) through (3)(a)(3) of H.R. 948 create a facially broad prohibition on the public display of Social Security numbers on the Internet, the requirement to use an individual's Social Security number as a password for access to any goods or services, and the display of Social Security cards on any membership or identity card. However, Section 3(c) grants the Federal Trade Commission open-ended authority to promulgate exceptions to the prohibitions contained within the bill. If exceptions concerning the display of Social Security numbers and requirement of their use as passwords are necessary, then they should be contained within the statute itself. Failing that, the authorization granted to the FTC should be narrowly tailored to areas in which exceptions are clearly needed. As currently formed, there is no way to know whether the exceptions will undermine the safeguards that are vitally important.

Although the purpose of the bill is, in part, to prohibit the sale and purchase of Social Security numbers, Section 4(a) only authorizes the FTC to create regulations to this end. Section 4(b)(1) requires the FTC to issue regulations but it provides little meaningful guidance on baselines standards the FTC should adopt. Furthermore, although Section 4(b)(2) appears to offer the Commission some substantive guidance, its language actually defines the ceiling for the FTC's rules rather than the floor. While the dual purposes of providing assurance that Social Security numbers are not to be used to commit fraud and to prevent undue harm are laudable, these should be the minimum requirements the FTC must meet under the act and should not define the boundary of the Commission's authority to regulate. Also troubling are the laundry list of required exceptions contained within Section 4(b)(3). Not only are the exceptions contained in Sections 4(b)(3)(A) through 4(b)(3)(F) requirements of any future FTC regulation, but also Section 4(b)(3)(G) gives the FTC open ended authority to create further exceptions pursuant to the general considerations in Section 4(b)(2). Despite its strongly worded purpose, the bill lacks adequate limitation on the sale or purchase of Social Security numbers and, instead, devotes more space to explicitly authorizing uses of Social Security numbers that were not originally intended.

Although it is laudable that the bill creates a right of action for states' attorneys general in Section 4(e)(2)(A), H.R. 948 fails to authorize a private right of action. Experience has shown that a private right of action is necessary in order to ensure vigorous enforcement of the law. While State and Federal governments are often consumed with pursuing other issues and may be unable to pursue every indiscretion to the fullest extent of the law, individuals are always motivated to vindicate their own rights. The possibility of expansive litigation indicates the importance of this problem; it does not provide a reason to restrict an individual's ability to protect his identity.

I should add further that EPIC has had significant success bringing privacy complaints to the Federal Trade Commission. In fact, it was our complaint regarding the

practices of the data broker ChoicePoint that led to the largest fine in the Commission's history.[64] Nonetheless, we would urge the Committee to include a private right of action, specifically where an individual or company misuses an SSN in violation of the Act. That will be critical to limit the problem of identity theft.

Finally, while a national standard may appear attractive, preempting state law will be a mistake. The preemption of state law will mean simply that certain practices that contribute to the crime of identity theft that are currently and appropriately outlawed by the states will become legal if this bill passes in its current form. Experience in other areas has made clear that a federal baseline for privacy protection is the best way to both create a national standard and to preserve innovation in the states.

VIII. Conclusion

There is little dispute that identity theft is one of the greatest problems facing consumers in the United States today. There are many factors that have contributed to this crime, but there is no doubt that the misuse of the Social Security and the failure to establish privacy safeguards are key parts of the problem. The Congress should pass strong and effective legislation that will limit the use of the SSN, that will provide effective means of oversight, that will not limit the ability of the states to develop better safeguards, and that will encourage the development of more robust systems for identification that safeguard privacy and security.

Thank you for your interest in this issue. I will be pleased to answer your questions.

[64] EPIC, *Past FTC Review of ChoicePoint Privacy Practices*, http://epic.org/privacy/ftc/google/#cpoint; *see generally* EPIC, *ChoicePoint*, http://www.epic.org/privacy/choicepoint/.