Testimony and Statement for the Record of

Marc Rotenberg
President and Executive Director, Electronic Privacy Information Center

Hearing on

Social Security Number High-Risk Issues

Before the

Subcommittee on Social Security
Committee on Ways and Means

U.S. House of Representatives
March 16, 2006
B-318 Rayburn House Office Building

Introduction

Chairman McCrery, Ranking Member Levin, and Members of the Subcommittee, thank you for the opportunity to testify on the high-risk issues surrounding Social Security numbers.

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 in1994, EPIC has participated in leading cases involving the privacy of the Social Security Number (SSN) 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] Last year, I testified on H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act of 2005 and urged Members to reject the use of the SSN as a national identifier and to ensure the development of adequate privacy and security safeguard to address the growing crisis of identity theft.[3]

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, 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. Recent efforts to expand employment verification programs based

---

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

[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"); Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, at a Joint Hearing on Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security (Nov. 8, 2001) *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC, at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims (Sept. 19, 2002) *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[3] Testimony of Marc Rotenberg, President, Electronic Privacy Information Center, at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005" before the House Judiciary Committee Subcommittee on Immigration, Border Security, and Claims (May 12, 2005) *available at* http://www.epic.org/privacy/ssn/51205.pdf.

upon SSN identification would turn the SSN into a national identifier, subjecting Americans to a national tracking systems and also heightening the risks of identity theft. There are additional risks associated with some of the technological features that the proponents of an "upgraded" Social Security card have suggested. As the New York Times reported yesterday, RFID chips that are being added to identity cards including the US passport, are apparently subject to computer viruses and other forms of attack.[4] These risks associated with the expanded use of the Social Security Number and identification cards underscore the importance of the hearing today.

History of SSN Use

The Social Security Number (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 canbe 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 enacted provisions to limit the uses of the SSN. 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 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 an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or

---

[4] John Markoff, "Study Says Chips in ID Tags Are Vulnerable to Viruses," New York Times, March 15, 2005.

[5] "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 125-35 (MIT 1973).

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.

The SSN as a National ID Number Erodes Privacy

Contrary to the clear intent of the Privacy Act, legislation considered this term has proposed to build the SSN and the Social Security card into a national ID. H.R. 98, for example, would create a *de facto* national identity card. Despite any disclaimers that the card was not to be used for identification, employers required to verify the information on the card (which would bear a photograph and a machine-readable unique identifier) would likely rely upon these "fraud prevention measures" as practical identification requirements. It is important to note that the SSN and its basic card are not intended to be used for authentication and identification purposes today, and yet far too many entities rely upon it for just those purposes. Adding the trappings of an identification document to it, including photographs and machine-readable technology, only reinforces the card's status as a badge of identity.

Furthermore, using the SSN for employment verification would necessarily require the building of a vast database of nearly all people employed within the country, which could be easily indexed and correlated with other databases via the SSN. It is precisely this use of the SSN that the drafters of the Privacy Act sought to prevent. H.R. 98 proposed that the database be available to Homeland Security for "any other purpose the Secretary of Homeland Security deems to be an the national security interests of the United States." This vague clause perfectly illustrates "mission creep," and highlights the risk that a national database, based on SSNs, established for one purpose could quickly be transformed into an open-ended system of national surveillance.

A mandatory, national index of all people employed within the U.S. would allow the tracking of individuals on an unprecedented scale. Each person applying for a job would be subject to a status determination by a government agency with each application. In essence, a person's life and livelihood would be determined by a database kept by the federal government—a database grounded in a flawed system of identification never intended for the purpose.

Identity Theft

Nor are the uses of a universal identifier limited to government uses. In fact, it is commercial enterprises that have made the SSN synonymous with an individual's identity. Despite the fact that the cards were never intended to be used for identification purposes, they are considered the "keys to the kingdom" for records about individual consumers.

The financial services sector, for instance, has created a system of files containing personal and financial information on nearly ninety percent of the American adult population, keyed to individuals' SSNs. This information is sold and traded freely, with virtually no legal limitations. This widespread use, combined with lax verification procedures and aggressive credit marketing that lead to widespread identity theft.

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. EPIC has detailed many of these cases in other testimony.[6]

The root of this problem is that the SSN is used not only to tell the credit issuer who the applicant is, but also to verify the applicant's identity. This would be like using the exact same series of characters as both the username and password on an email account. The fact that this practice provides little security should not be a surprise.

The printing of SSNs on government-issued drivers licenses provided yet another opening for identity thieves. A thief who stole your wallet could also easily steal your identity, with name, address, diver's license number, and SSN in one easy place. Congress recognized this threat and in the Intelligence Reform and Terrorism Prevention Act of 2004, prevented the printing of SSNs on drivers licenses and other government-issued ID.[7]

International Experiences

The debate on national identification cards is not restricted to the United States. Fierce debates have erupted in other countries over the adoption of national ID cards. The problems presented by such cards in the UK, France, and many other nations are the same problems that we would face here—convenient categorization of individuals' records, to be used or abused by governments or those who obtain access to government records.

The protests against the UK national ID cards are strong, and from esteemed sources such as the London School of Economics[8], yet they address a system that is even

---

[6] *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).

[7] Pub. L. No. 108-408 §§7211-7214, 118 Stat. 3638, 3825-3832 (2004).

[8] London School of Economics, The Identity Report: an assessment of the UK Identity Cards Bill and its implications (2005) *at* http://is2.lse.ac.uk/IDcard/identityreport.pdf.

less problematic than one that could use the SSN as a national ID. In the UK, for example, the national ID card would be a voluntary document. And in Ireland, a proposal to establish national was recently rejected.[9] Here in the US, SSNs are most frequently assigned at birth. We would be putting in place a system mandating ownership of a machine-readable photo ID, a step that other parts of the world, even those less opposed to government interference in personal affairs, seem loath to take.

Measures to Prevent Fraud

The need to present such a card at every employment encounter, and possibly also for homeland security purposes, would also likely increase the need to carry the card on one's person, rolling back the benefits achieved by taking the SSN off of driver's licenses. The reason that the SSN can so easily be used for fraud is not that the card lacks anti-counterfeiting measures; it is the fact that the card is being used as an identifier in so many contexts that it should not be. Efforts to protect the SSN and its holders should therefore be focused upon limiting its uses and disclosures.

Several states have, in recent years, established new privacy protections for SSNs. These laws demonstrate that major government and private sector entities can still operate in environments where disclosure and use of the SSN is limited. They also provide examples of protections that should be considered at the federal level. For example, Colorado, Arizona, and California all have laws that broadly restrict the disclosure and use of the SSN by both government and private actors. These laws encourage agencies and businesses to use different identifiers for their specific purposes, reducing the vulnerability that the disclosure of any one identifier may create.[10] Arizona's law also prohibits the printing of the SSN on material mailed to Arizona residents, reducing the threat of fraud from intercepted correspondence.

Other states, including New York and West Virginia, have statutes that limit the use of the SSN as a student ID number.[11] This reduces the vulnerability of students to identity theft and protecting the privacy of students whose personal information is collected in databases, and whose grades are often publicly posted, indexed by their student ID numbers.Similar laws exist in Arizona, Rhode Island, Wisconsin, and Kentucky.[12]

---

[9] EPIC prepares an extensive annual survey of international developments concerning privacy protection, including the debates over identity documents. See *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (EPIC 2004), available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82586&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004#_Toc396491834 ("Identity systems").

[10] Colo. Rev. Stat § 24-72.3-102; Ariz. Rev. Stat. § 44-1373; Cal. Civ. Code § 1798.85.

[11] N.Y. Educ. Law § 2-b; W. Va. Code Ann. § 18-2-5f.

[12] Ariz. Rev. Stat. § 15-1823; R.I. Gen. Laws § 16-38-5.1; Wis. Stat. Ann. § 36.11(35); Ky. Rev. Stat. Ann. § 156.160.

Congress and this Committee has likewise moved to protect the SSN; just this session, Chairman Shaw and many other members of this Committee introduced legislation that would have added protections on a federal level. We hope that the Committee will be able to act on these proposals this session

These various proposals all tend towards limiting the uses of the SSN, in notable contrast to proposals that expand SSN uses and thus expand individuals' vulnerability. We therefore urge the Committee to regard cautiously any attempt to expand the use of the SSN beyond its already overextended purposes.

Conclusion

The expanded use of the Social Security Number is fueling the increase in identity theft in the United States and placing the privacy of American citizens are great risk. The widespread use of the SSN has made it too easy for government agencies, businesses, and even criminals to create detailed profiles of individuals Americans. Congress wisely sought to limit the use of the Social Security Number when it passed the Privacy Act of 1974, and the states have since established additional safeguards. While new techniques may address some of the security and privacy issues associated with the expanded use of the Social Security card, it clear that these techniques also create new privacy and security risks. We urge the Committee to consider very carefully the high-risk issues associated with the use of the Social Security Number. Every system of identification is subject to error, misuse, and exploitation.