

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Testimony and Statement for the Record of

Marc Rotenberg
President and Executive Director, Electronic Privacy Information Center

Hearing on

Social Security Numbers in Commerce:
Reconciling Beneficial Uses with Threats to Privacy

Before the

Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce

U.S. House of Representatives
May 11, 2006
2123 Rayburn House Office Building

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for the opportunity to testify today on Social Security Numbers in commerce and how best to reconcile beneficial uses with threats to privacy.

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 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.² Last year, we 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." A number that was created for a specific, limited purpose has been transformed for additional, unintended purposes, sometimes with disastrous results. The pervasiveness of the SSN threatens privacy and the financial security of Americans. For example, SSNs are routinely used to both identify and authenticate an individual, a deeply flawed security practice.

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>.

SSNs are also used to build detailed profiles on American consumers, linking together records that might otherwise be difficult to match. Without the SSN, businesses would have to be more forthcoming with individuals about the sources of information that are obtained and the profiles that are created. However, the SSN makes it possible to create profiles that are not only detailed but also secretive. As a consequence, consumers are able to exercise less control over their personal information held by others. Absent an explicit statutory protection, they have no idea what information about them is collected, how it is used, or to whom it is disclosed.

The privacy risks associated with the creation of the SSN have been well understood for a long time. Although Congress successfully limited some uses of the SSN by federal agencies with the passage of the Privacy Act in 1974, since that time Congress has largely failed to establish the necessary safeguards to protect American consumers.

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 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, Computer, and the Rights of Citizens*, the report that provided the basis for comprehensive privacy legislation in 1974, 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."⁴

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of the widespread use of SSNs as universal identifiers, and enacted provisions to limit

⁴ "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).

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 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.

However, the Privacy Act failed to limit the use of the SSN by the private sector as the 1973 report had urged. Credit reporting agencies, marketing firms, and more recently, data brokers to build detailed profiles on American citizens exploited this loophole. As a consequence, consumers have experienced the extraordinary problem of identity theft.

Identity Theft

Commercial enterprises have made the SSN synonymous with an individual's identity. Despite the fact that the SSN was 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 has 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.⁵

⁵ 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).

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, driver'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.⁶

States are Taking the Lead on SSN Privacy

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.⁷ 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.⁸ 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.⁹

Of course, we would welcome strong legislation in Congress that would limit the use of the Social Security Number in the private sector and help safeguard the privacy interests of American consumers, but the bills now pending before the Committee have been so watered down it is not clear that they would provide much actual benefit. Many exceptions have been created to permit business to continue to collect and use the SSN for a wide range of commercial activities. There are also problems with the lack of effective enforcement. And the bills generally provide less protection than comparable state measures.

⁶ Pub. L. No. 108-408 §§7211-7214, 118 Stat. 3638, 3825-3832 (2004).

⁷ Colo. Rev. Stat § 24-72.3-102; Ariz. Rev. Stat. § 44-1373; Cal. Civ. Code § 1798.85.

⁸ N.Y. Educ. Law § 2-b; W. Va. Code Ann. § 18-2-5f.

⁹ 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.

Possible SSN Privacy Legislation

I would like today to propose a simple approach to safeguarding privacy and limiting the misuse of the Social Security Number and that is to recommend legislation that would prohibit the collection and use of the Social Security Number by a commercial organization where there is no legal authority to do so. Simply stated, if Congress determined that it was necessary to authorize the use of the SSN in the private sector, as it did when it chose to make the SSN the Tax Identification Number, then a commercial firm would have the legal authority to collect and use the SSN consistent with that statutory purpose. But where there is no legal authority to collect an individual's SSN, the commercial firm would be prohibited from doing so. This would change the default on the use of the SSN and help ensure that the number was used only for appropriate purposes.

You could also, if you wish, apply the approach set out in section 7 of the Privacy Act by requiring private sector organizations that seek to collect an individual's SSN to inform that individual whether the disclosure of the SSN is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of the individual's SSN. Many privacy notices have become extraordinary complex and are routinely ignored. But the original notice for the collection and use of the SSN set out in the Privacy Act of 1974 would actually be very helpful for consumers who are trying to safeguard their privacy.

Either approach would provide meaningful limitations on the use of the SSN, reduce the risk of identity theft, and help restore consumer privacy. These are also the approaches consistent with the Privacy Act of 1974 and the 1973 report that provided the basis for that landmark law.

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 at 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 by federal agencies when it passed the Privacy Act of 1974, and the states have since established additional safeguards. Still it is clear that the problem of the misuse of the Social Security Number is on the rise.

Effective privacy legislation for the SSN in the commercial sector could be based on either requiring businesses to have legal basis to collect and use the SSN or by applying Section 7 of the Privacy Act to commercial entities.