Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, Electronic Privacy Information Center
Adjunct Professor, Georgetown University Law Center

Joint Hearing on

SSNs and Identity Theft

Before the
Subcommittee on Oversight and Investigations
Committee on Financial Services
and
Subcommittee on Social Security
Committee on Ways and Means

U.S. House of Representatives
November 8, 2001
2138 Rayburn House Office Building

My name is Marc Rotenberg. I am the executive director of the Electronic Privacy Information Center, a public interest research organization based here in Washington. 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 written briefs in two of the leading cases involving the privacy of the Social Security Number (SSN), and I have had the pleasure of testifying before the Subcommittee on Social Security this past May on the use and misuse of the Social Security Number.

I appreciate the opportunity to testify this morning on one of the unfortunate results of the misplaced reliance on SSNs as universal identifiers. The problem of "identity theft", particularly of the deceased, cannot be solved by sharing SSN data more rapidly or other such stopgap measures. The problem lies rather in the dramatic expansion of the use and collection of the SSN that Congress should try to limit. I will briefly review the efforts to regulate the use of the SSN, discuss some of the problems with universal unique identifiers, 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.

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.

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 are seeking to correct 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."[1]

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

[1] *Records, Computers and the Rights of Citizens* at 135.

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."[2] 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 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.

Financial Services Use of SSN

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 learn 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. Information is freely sold and traded, virtually without legal limitations.[3]

It is the financial service industry's misplaced reliance on the SSN, lax verification procedures and aggressive marketing that are responsible for the financial consequences of "identity theft."[4] Congress must encourage the industry to develop alternative, and less intrusive systems of record identification and verification. We have also suggested to this Subcommittee before that Congress fund a National Research Council study to explore new techniques that will enable record management while minimizing privacy risks. Moreover, the misuse of death records underscores the need for consumers to have easy access to view and correct their credit reports, and to have the ability to control the use and dissemination of personally identifiable information.

---

[2]

> (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).

[3] Komuves at 557.

[4] See for example the GAO Report that details the high cost and difficultly involved with preventing social security card fraud and therefore its current unreliability as a unique identifier. See also the SSA's Office of Inspector General reports and testimony on the misuse of SSN. [http://www.ssa.gov/oig/hotreports.htm]

Social Security Administration's Death Master File

The Death Master File is publicly available from the Social Security Administration (SSA) for a little under $1,800 for a single issue ($6,900 for a quarterly subscription with monthly updates). Anyone can buy 60 million electronic records from the SSA on all Americans (and others with SSNs) that have died. These records contain important personal identifiable information, including the name, social security number, date of birth, date of death, state or country of residence, ZIP code of last residence, and ZIP code of lump sum payment to the decedent's beneficiary. These records are also accessible for free on the web at places like Ancestry.com. The records have over a 3% error rate, and provide information chiefly on those who died after 1960.

It is remarkable that such a data goldmine is made publicly accessible by SSA and is a sobering reminder of the urgent need to restrict access to sensitive personally identifiable information. Rather than focusing attention on how these records can be transmitted more rapidly and accurate to commercial and private users, Congress must first consider placing limitations on the use and access to such data. Unscrupulous users of this database for instance might be able to exploit the recently bereaved or take advantage of their changed financial circumstances. Separate from what residual privacy concerns might be there for the recently departed, it is important to appreciate the effect such disclosure has on the survivor's privacy where their spouse's or parent's name, SSN and location is made freely available. The database might arguably be of some help for those engaged in historical research, but the terms and conditions of such use can be regulated to protect the privacy of survivors.

It also seems obvious that the more widely disseminated this information is the more opportunities for financial fraud and identity theft will arise. If Congress chooses to make the Death Master File more readily available to the private sector, then I urge to adopt corresponding privacy rules that will limit the opportunities for abuse.

Conclusion

As I suggested in my testimony in May to this Subcommittee, I believe that 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. The prospect that the Death Master File will be made more widely available outside of the federal government further underscores the need for legislation in this area.

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 and dissemination of the SSN and that encourages organizations to develop alternative systems of record identification and verification. It is important to emphasize the unique status of the SSN 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, it's entirely inappropriate use as a national identifier for which it is also inherently unsuitable, and the clear history in federal statute and case law supporting restrictions, it is fully appropriate for Congress to pass legislation.

I am grateful for the opportunity to testify this morning and would 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 an 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)

GAO Report, "Mass Issuance of Counterfeit-Resistant Cards Expensive, but Alternatives Exist," (August 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)

Marc Rotenberg, *Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* (EPIC 2001)

Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizen*s (MIT 1973) (Social Security Number as a Standard Universal Identifier and Recommendations Regarding Use of Social Security Number)