
PRIVACY TIMES

EDITOR: EVAN HENDRICKS

**TESTIMONY OF EVAN HENDRICKS
EDITOR/PUBLISHER
PRIVACY TIMES**

**Before The Subcommittee On Oversight & Investigations
House Committee On Financial Services**

**Before The Subcommittee On Social Security
House Ways and Means Committee
November 8, 2001**

Madame Chairwoman, Mr. Chairman and Members of the Subcommittees, thank you for this opportunity to testify on the important issue of preventing the misuse of Social Security numbers (SSNs) of the deceased.

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.

As a Sports fan, I often hear that "If you do the little things right, you get the big things right."

Unfortunately, when it comes to SSNs, as a nation, we have over the years made a series of bad decisions. The underlying mistake has been to expand the use of the SSN beyond that for which it was created: the numbering of personal accounts for the collection of taxes and benefits in the Social Security program. Since 1936, when the number was first established, Congress

Privacy Times PO Box 21501 Washington, D.C. 20009 (301) 229 7002
www.privacytimes.com evan@privacytimes.com

has authorized its use for additional purposes, including drivers' licenses, financial records and Federal, State and local governmental agencies. In addition, many private companies -- insurers, health care organizations, universities and health clubs -- use the SSN as their primary personal ID number for customers.

Thus, in many significant ways, the SSN has become a *de facto* national identifier. This is of course is not consistent with the U.S. Government's original promise to the American people that the SSN would not be used for identification purposes. It also means that as a society, we have lost considerable control over the SSN. They are available in too many places: Web sites, court records and bulletin boards. They are available for sale from information brokers. They are vulnerable to unauthorized access, use and even sale wherever they are stored, be it a personnel department, a government database or a Web site.

The SSN is the first number that is sought by (1) credit-identity thieves; (2) by people trying to hide their true identities, like terrorists; and (3) people trying to enter or remain in the United States in violation of our immigration laws.

These factors, along with many others, point to the urgency of enacting legislation to protect the privacy of SSNs, and to support efforts by Chairman Shaw and other Members to enact such legislation. My May 22 testimony before Chairman Shaw's Subcommittee, in which I also called for comprehensive privacy legislation and oversight, is available at <http://waysandmeans.house.gov/socsec/107cong/5-22-01/5-22hend.htm>.

The New Paradigm: Identity Theft

Few people realized that the failure to protect the privacy of personal data and the SSN has made possible what is becoming 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."

Thanks to fine reporting by Robert O'Harrow, Jr. of the *Washington Post*, we know that identity thieves regularly use stolen credit card numbers to buy SSNs and other personal data from information brokers and then use the information to commit credit fraud.

Some of the key solutions to identity theft include prompt and regular consumer access to his or her credit report and or/notification to the consumer of new activity on the credit report, stricter duties on CRAs to ensure that an innocent consumer's credit report is not disclosed in response to a credit application by an imposter, and wider use of "disposable" or "one-time" credit card numbers.

According to the Privacy Rights Clearinghouse and the Identity Theft Resource Center, another disturbing method of operation is for identity thieves to gather news about recently deceased persons, either from local agencies that issue death certificates, or from the obituaries, and use the information to commit credit fraud.

These groups reminded me of press reports that one woman stole the identity of a victim she knew who died in the World Trade Center attack and committed credit fraud. Also, a California limousine driver, who was to pick up a man who died on a hijacked Sept. 11 jet, stole the man's identity and committed credit fraud.

SSNs Of The Deceased

In addressing the issue of the SSNs of the deceased, it's important to consider a fundamental flaw in the current system: While the use of and reliance upon the SSN is widespread (making it a *de facto* ID number), the system for issuing it, protecting it and expiring the SSN is antiquated, relative to advanced information technology.

The Social Security Administration maintains a "Death Master File," consisting of 60 million names and SSNs of deceased persons, available for sale by the National Technical Information Service (www.ntis.gov). But, as the NTIS Web site states, "The SSA does not have a death record for all persons; therefore, SSA does not guarantee the veracity of the file. Thus, the absence of a particular person is not proof this person is alive."

Although it is not entirely clear how SSA gathers information on deceased persons, it appears that the information comes from a variety of sources, including SSA beneficiary records, local government agencies that issue death certificates and relatives of the deceased. But the SSA's system can be described as "hit-or-miss," leaving the Death Master file incomplete.

It appears that a thorough overhaul of this system is necessary, particularly given the growth in the abuse of the SSNs of the deceased. What is needed is an automated system by which the local governmental agencies in charge of issuing death certificates can instantly report to SSA the names and SSNs of deceased persons. SSA, in turn, can report these names and SSNs to the three major credit reporting agencies (CRAs). The CRAs would then be responsible for ensuring that an identity thief did not exploit a deceased person's SSN for financial gain. Legislation could help facilitate creation of such a system, both by providing legal authorization and the necessary appropriations. Such legislation should specify that the system be created

solely for the purpose of ensuring accuracy of information systems that maintain SSNs of the deceased.

Privacy, The Purpose Test & Real Oversight

We live in an Age in which a plethora of personal information is available about all of us from a wide variety of sources. Protecting privacy in the Information Age does not mean shutting down all systems or locking up all personal data -- that will never happen, nor should it. An important aspect of protecting privacy in today's environment is defining the purposes for which information may be used. That is why the Fair Credit Reporting Act, the first information privacy law (1971, amended in 1996) defines the "permissible purposes" for which credit reports may be used. And, like the FCRA, privacy laws must create penalties to deter misuse of personal data and remedies for individuals whose privacy is invaded.

Another important aspect in the protection of privacy is oversight and enforcement. The United States lacks what every other Western nation has: An independent national office to oversee and enforce privacy law. Other nations get great value from their Privacy Commissioners, who typically report to Parliament, receive complaints from citizens, investigate, conduct audits of organizations' information systems, study new technologies, and serve as a public resource. The U.S. Privacy Protection Study Commission, a bipartisan panel created by the Privacy Act of 1974, recommended such an office in 1976.

Privacy is a very broad issue, affecting every aspect of our society: finance, medicine, employment, commerce, communications, law enforcement and counter-intelligence. It will be difficult if not impossible to ensure that privacy rules are administered effectively across these sectors without appropriate direction. An independent Office of Privacy Commissioner, created by statute and reporting to Congress, is the appropriate entity to provide that direction.

Madame Chairwoman, Mr. Chairman, again, thank you for this opportunity to appear before the Subcommittee. I'd be happy to answer any questions.