

February 24, 2007

YOUR MONEY

Think Your Social Security Number Is Secure? Think Again

By [DAMON DARLIN](#)

It should come as little surprise that Social Security numbers are posted on the Internet. But, says Betty Ostergren, a former insurance claims supervisor in suburban Richmond, Va., who has spent years trolling for them, “people are always astounded” to learn that theirs is one of them.

Mrs. Ostergren, 57, has made a name for herself as a gadfly as she took on a lonely and sometimes frustrating mission to draw attention to the problem. With addresses, dates of birth and maiden names often associated with Social Security numbers, she said, they are a gift to data thieves.

But in the last few weeks, Mrs. Ostergren’s Web site, [The Virginia Watchdog](#) — with the help of lobbying from an unexpected ally, America’s farm bureaus — is having an effect.

One by one, states and counties have started removing images of documents that contain Social Security numbers, or they are blocking out the numbers. Four states, including New York, have removed links to images of public documents containing Social Security numbers.

Snohomish County, Wash., for example, said Wednesday that 61 types of documents, including tax liens and marriage certificates, would be blocked. (The documents are supposed to remain public at courthouses or state offices.)

Last week, the Texas attorney general, Greg Abbott, issued a legal opinion that county clerks would be committing a crime by revealing Social Security numbers on the Internet.

“I am almost in a celebratory mode,” said David Bloys, a retired private investigator in Shallowater, Tex., who also highlights the public records issue on his Web site, [NewsforPublicOfficials.com](#).

For people wondering if they should be worried about the security of their own numbers, there is a new tool to help them.

TrustedID, a company that sells services to consumers to give them more control over who sees their credit reports, has compiled a database of compromised numbers that could already be traded or sold on the Internet.

It has created an online search tool, [StolenIDSearch.com](#), where people can check at no cost to see if their number is one that is in a too-public domain.

TrustedID said that about 220,000 people have tested their numbers in the three weeks since the site has been open to the public.

The Social Security number remains the personal identifier not only for government documents, but for credit applications and medical records, as well as video and cellphone stores.

“In the commercial world it is ubiquitous when credit is offered,” said Chris Jay Hoofnagle, a privacy advocate and senior fellow of the Berkeley Center for Law and Technology at the [University of California](#), Berkeley. “It all flows from the credit system and it flows very far.”

Even though Americans are told to protect their Social Security number to prevent identity theft, that is a tall order. The [Social Security Administration](#) says its card “was never intended and does not serve as a personal identification document.”

But that has not been true about the number almost from outset. The Social Security numbers that were first handed out in November 1936 as a means for the federal government to track payments to the retirement system was soon used for other purposes. It helps tracks payroll, loan payments, financial transactions and income taxes.

It is necessary for anyone seeking public assistance, like food stamps, or registering for the draft. Congress decreed it be recorded on records including professional licenses, marriages licenses and divorce decrees to better track scofflaws of child support orders.

The Social Security number took on a second role. It allowed collectors of data to link pieces of information together, like a driver's license record, credit report data, and the information on the warranty card for a toaster. That is a useful tool for marketers and just as useful for criminals.

It was only in 2004 that Congress prohibited states from using the Social Security number on drivers' licenses. Yet the databases with those numbers still exist and are still sold. Until 2001, states could sell lists with those numbers, which means that most anyone 22 years or older probably will have their name, address, phone number and Social Security number in private databases.

The nine-digit string took on a third role — as a password that was supposed to protect all that private information from snoops and criminals. But its ubiquity defeats that purpose, Mr. Hoofnagle said. "It will pass when the business community no longer needs a Social Security number," he said.

The Social Security Administration's Office of Inspector General said that 16 percent of the 99,000 fraud cases it investigated in the 12-month period that ended Sept. 30 involved the misuse of Social Security numbers. One involved an identify theft ring in central Florida. Twelve people were convicted, sentenced to prison and ordered to repay more than \$2 million.

About 16,000 incidents are not a lot considering that 240 million numbers are currently in use, and certainly credit card number theft and fraud is much more pervasive.

But credit card numbers rarely are exposed on documents in public view. And if a credit card is stolen or misused, obtaining a new one is a fairly simple process. A new Social Security number is rarely granted. (Indeed, one is limited to three replacements of the green paper Social Security card in a year and 10 over a lifetime.)

Social Security numbers are routinely traded and sold by thieves over the Internet like credit card numbers, says Panos Anastassiadis, chief executive of Cyveillance, an Arlington, Va., company that monitors online fraud attempts for major financial institutions. His company has found caches of them in Web chat rooms where they are offered as samples by criminals selling even larger lists.

They are sometimes obtained by "key logging" software surreptitiously installed on home computers to record what is typed. Some come from so-called phishing attacks in which people are misled into entering the data on fake Web sites of banks or utilities.

The numbers are also out in the open. "People think it is the banks, but banks are very secure," Mr. Anastassiadis said. "The problem is every dentist's office has Social Security numbers. Every doctor's office has them. How secure are these?"

It has been Mrs. Ostergren's near-obsession to answer that question.

Few things delight her more than finding a number belonging to a celebrity because it draws attention to her cause.

"Oh, my Lord!" she exclaimed recently as she stumbled upon the Social Security number of a member of the boldfaced set as she demonstrated how New York state Web sites display documents containing names, addresses and Social Security numbers. "Let me download this one. This is [Donald Trump](#)'s number. I can't wait to tell him."

Mrs. Ostergren never got through to Mr. Trump to confirm whether the nine-digit identifier was indeed his, but she has found and tried to notified others, including Kelly Ripa, the actress and talk-show host; [Jeb Bush](#), the former governor of Florida; [Porter Goss](#), the former [C.I.A.](#) director; and scores of state legislators, and posted the link to them on her site. (New York later removed links to public documents.)

She has found Social Security numbers on tax liens on the official site of Maricopa County in Arizona. In Florida, as in many states, they appear on a document people sign when they buy furniture or other merchandise on credit.

Mrs. Ostergren wants the documents taken off the Web, and she applies pressure by using the people whose numbers she finds. "I've been calling people and telling them that they are exposed," Mrs. Ostergren said. "It is not very hard to find the numbers," she said. "They are exposed everywhere."

Her Web site may be cluttered with so many typefaces that it resembles a ransom note, but she seems to be having an impact. In the last month she found a pressure point: farmers.

Their numbers show up on Uniform Commercial Code filings when they buy machinery or supplies on credit. She showed state farm bureau leaders their numbers; they contacted their state legislators. She has also found common cause with other gadflies like Mr. Bloys.

She has had her share of setbacks as well. Several state legislators tried to ban her from posting information about their personal data that appear in public records. She wins no fans among legitimate companies who sell databases. Removing the data from the Internet slows down their ability to collect public information, but does not stop it.

“There are a lot of people in the data brokerage business who don’t like what I do,” she said.

[Copyright 2007 The New York Times Company](#)

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)