



[Comments](#) 8 | [Recommend](#)  0

Privacy fears aired about safety of Social Security data

12:00 AM CDT on Sunday, August 9, 2009

By BOB MOOS / The Dallas Morning News

bmoos@dallasnews.com

David Leopard of Richardson has devoted a good part of his retirement to helping seniors guard against identity theft.

But even this former FBI agent and corporate security executive isn't sure what to make of a research team's claim that it can predict most, and sometimes all, of an individual's nine-digit Social Security number from publicly available information.

"I'm not familiar with how anybody can make that kind of prediction, but I do know it's become far too easy to get hold of someone's Social Security number," said Leopard, who has given dozens of presentations on identity theft to senior groups throughout the Dallas area. "Why would a crook have to resort to guesswork? All he needs, unfortunately, is a little ingenuity."

Still, Alessandro Acquisti, an associate professor of information technology and public policy at Carnegie Mellon University, and Ralph Gross, a postdoctoral researcher, have rattled some data-security experts with their recent assertion that they can make an educated guess about someone's Social Security number if they know the person's date and place of birth.

Finding patterns

Without disclosing exactly how they did it, the researchers said they relied on Social Security's "death master file," a public database of the names and Social Security numbers of deceased individuals. By examining the list of dead people, Acquisti and Gross discovered statistical patterns they then used to fathom the system Social Security uses to assign numbers to living people.

The researchers said their predictions were most accurate for people born after 1988, when most Americans began receiving their numbers shortly after birth, and for individuals from less-populous states.

Acquisti explained his research at a recent national conference on privacy in Las Vegas. Because many businesses continue to use Social Security numbers as passwords or for other forms of authentication, the predictability of the numbers increases the risk of identity theft, he said. Such theft already accounts for \$49.3 billion in fraudulent charges a year.

Social Security has played down the significance of the Carnegie Mellon team's work, noting that the agency's general method for assigning numbers has been known for years. Still, Social Security said it's developing a system of randomly assigning numbers to make such discoveries more difficult.

Cause for concern

Even ignoring Acquisti and Gross' research, there's still cause for the public to be concerned about the privacy of Social Security numbers, Leopard said. When the government first issued the numbers in 1936, it assured the public that they would be used strictly for agency business such as figuring retirement benefits. But over the decades, they've become a de facto national ID.

"The business use of Social Security numbers has become almost ubiquitous," he said. "Many of us are required to present them as proof of identity when applying for credit, insurance and jobs. But the more we use them, the more vulnerable we become to identity thieves. And once they get their hands on them, they can open all kinds of accounts in our names."

Businesses haven't always been careful in handling Social Security numbers. The Texas attorney general has sued about a dozen companies in the last couple of years after workers carelessly disposed of customers' personal records, said spokesman Tom Kelley.

A 2005 Texas law requires business to properly dispose of documents containing sensitive information, he said.

What's particularly frustrating is that the government itself has contributed to the ID theft problem, said Lynda Ender, director of advocacy for the Senior Source in Dallas. Despite the growing threat, 45 million Medicare cards continue to display their beneficiaries' Social Security numbers, she said. Legislation to change the practice has been introduced in Congress.

"Seniors also become their own worst enemies when they hand over their Social Security numbers to strangers without thinking," said Suzanne Cobb, who supervises a program at the Senior Source that helps older adults manage their money. "Con artists call them, win their confidence with some tall tale and then trick them into disclosing their personal information."

Guarding your privacy

Leopard urges his audiences to take a hard line when asked for Social Security numbers.

"Never give out your personal information to an unsolicited caller," he said. "And even when you're the one approaching a business, don't be so quick to hand over your number if requested. "First, ask if it's required and then ask how the business intends to use it and protect it. If you're not satisfied, ask to talk to a manager about making an exception."

There are valid reasons for requesting someone's Social Security number, such as for government benefits or tax purposes, said Linda Foley, founder of the Identity Theft Resource Center. But if businesses are forced to field more questions from consumers, they may have more incentive to develop another ID system, she said.

Foley said a new federal law will also require financial institutions and creditors to pay closer attention to preventing identity theft. "Those businesses will have to create policies to identify, detect and respond to red flags indicating ID theft," she said.

"The use of Social Security numbers has spiraled out of control," Foley said. "It's time to apply more safeguards."

