Privacy Journal
AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE
PO Box 28577
Providence RI 02908

Statement on
SOCIAL SECURITY NUMBER PRIVACY ACT BILL
H-5202
February 7, 2011, House Corporations Committee

Use of stolen Social Security numbers is the major instrumentality of identity theft.

There are two major forms of identity theft. One involves using a stranger's SSN or other forms of identity to secure identity documents in the name of the victim so that the imposter may qualify for immigration documents, government benefits, a job, or even medical care. Undocumented immigrants often commit this form of identity theft. A victim's ID sometimes is left at a crime scene by the imposter.

The other form involves an imposter applying for credit using the name and Social Security number of an individual. To make this work, of course, the imposter must use an address of his choosing – to get the products and to make sure that the victim does not get the retailer's bills. This accounts for an estimated 60 percent of identity theft. It is usually more harrowing for the victim because it prevents the victim from using credit accounts and creates negative information on the victim's credit report, which are time-consuming and difficult to remove (even though federal law provides the right to get removal). It is caused because credit bureaus are permitted to match an incoming credit request from a retailer with a credit report in its files **if only the Social Security numbers match**. (This outmoded practice should be prohibited by state law.)

Therefore, Rhode Island enacted General Laws 6-13-15 to prohibit merchants from recording Social Security numbers on checks they receive; 6-13-17 to prohibit retailers and others from requiring that consumers provide an SSNs in a transaction; 6-13-19, to prohibit requiring SSNs as a condition of getting discount cards; and 6-48-8, to prohibit government agencies and businesses from requiring SSNs for various non-Social Security purposes. **This serves to reduce the number of Social Security numbers in circulation and in storage**, where, as we know, they are subject to disclosures by hacking, accident, or carelessness.

But some entities want to continue to ask for part of a Social Security number, so that they can use the last four digits to match a record already in their files or more likely to lead the consumer into believing that he or she can be tracked down in the event of a bad transaction. This violates the spirit of the state laws cited here. The amendments suggested in this session would simply make it clear that gathering even part of an SSN, like last four digits, violates the laws.

With these amendments, merchants would need to abandon use of the last four digits of the SSN as a matching device, which they should do anyway – using instead address, age, date of birth, telephone numbers, email address, PIN numbers or other less incriminating indicators).

There is danger in releasing even part of a SSN, because the nine digits are not anonymous. The first three indicate the state in which the card was issued (strictly speaking, the Zip code from which an application for a number was sent). Rhode Islanders generally are issued digits between 035 and 039, not a wide span of digits. This is no secret. The "area numbers" are listed by the Social Security Administration on the Internet.

Thus, with the last four digits – as some Rhode Island merchants and agencies are requiring – and the first three digits known by educated guess, a clever fraudster could use computer techniques to make an educated guess at the middle two digits. That means that with the state of residence and the last four digits alone, a fraudster can make an educated guess at the complete Social Security number. He would be helped by the fact that the middle two digits have been issued by the Social Security Administration to indicate roughly in what year the number was issued. The middle two digits do not represent the year of issue, but a table on the Internet indicates the time period for each number combination,

http://www.howstuffworks.com/framed.htm?parent=question719.htm&url=http://www.ssa.gov/employer/stateweb.htm

By knowing the age of his or her victims – not a hard item to find on Facebook – the fraudster could significantly reduce the chances of error in finding the middle two digits.

In addition, a by-product of the current laws in Rhode Island is that they diminish **the dehumanization that people experience when they are asked for a number and labeled with a number.** This effect is defeated by allowing merchants to collect the last four digits. The laws also allow some sense of mind for members of some religious sects who fear the enumeration of human beings as against Biblical warning. This too is defeated by allowing merchants to collect the last four digits.

Rhode Island was an early leader in protecting Social Security numbers, with the nation's first law limiting their use in the private sector, 6-13-15, and it has remained so ever since.

With the suggested amendments, the legislature will be closing a loophole that was not anticipated in the original legislation in 1993.

Submitted February 8, 2011, by Robert Ellis Smith, attorney and publisher of Privacy Journal newsletter, PO Box 28577, Providence RI 02908, 401/274-7861, www.privacyjournal.net.

See attaché excerpt from Small Wars Journal

The Military's Cultural Disregard for Personal Information

by Gregory Conti, Dominic Larkin, David Raymond, and Edward Sobiesk
From **Small Wars Journal**, December 6, 2010

" Identity theft is not simply an inconvenience; it can lead to long-term financial and legal difficulties for individuals and families. In forward-deployed locations such as Iraq and Afghanistan, the distraction caused by identify theft can directly affect combat readiness as service members attempt to recover from these crimes. What makes matters worse it that Soldiers, Sailors, Airmen, and Marines face an increased likelihood of being targeted due to the manner that many military organizations treat individuals' Social Security numbers, dates of birth, and other Personally Identifiable Information (PII). There are numerous recent examples of deployed service members being victims of identity theft." Page 1

"When we randomly choose a password that is, say, 9 characters long, there are 10^{12} to 10^{16} possible results, depending on the use of upper and lower case characters, numbers, and common symbols. Unfortunately, the Social Security number is no password. We change our passwords every three to six months, but our Social Security number is with us for life. Far from being a 9 digit random number with a billion possibilities, parts of a Social Security number are based on easily guessable patterns related to location and date of birth. In fact, two Carnegie Mellon University researchers found that they can reliably guess the first five digits of the Social Security number given only those two pieces of information [20]. The researchers state that **the relatively hard part of the problem is guessing the four digits of the Social Security number (often called the "Last 4"), which may take them several hundred tries."** Page 6

"Determining the first five digits of an individual's SSN is not difficult. For someone trying to abuse your SSN, the hard part is determining the last four digits. Therefore, the belief that it is safe to disclose the last four digits of one's Social Security number or alternatively to use these digits as a form of password is fundamentally incorrect, but nevertheless common practice."

http://smallwarsjournal.com/blog/journal/docs-temp/615-conti.pdf Page 7