About
Membership
Government Affairs
Respondent Coop
Information on Demand
CMOR e-Newsletter
What Is Research?
Contact Info

Government Affairs

CMOR :: GA Articles :::

Congress Looks at Social Security Numbers and Identity Theft
By Robert Genovese, Legislative Intern, and Howard Fienberg,
Director of Government Affairs
August 2007

Researchers do not often collect social security numbers (SSNs) for research purposes, except in limited cases, such as financial research. However, because SSNs play a sizeable role in cases of identity theft, the general public and legislators always look for ways to target the use and misuse of SSNs. This month's Legislative Update is packed with legislative proposals aimed at just that issue.

That is one of the reason CMOR attended a hearing of the Social Security Subcommittee of the House Ways & Means Committee on June 21 – a hearing that should be of interest to the profession. The Subcommittee has held 16 such hearings in the last seven years, with the hope of enhancing the privacy and security of the SSN and halting identity theft through the illegal appropriation of SSNs.

Congressional Hearing
The first panel of witnesses included **Senator Chuck Schumer** (D-NY), who stressed that the public exposure of SSNs should not go unchecked. He advocated a solution requiring that all organizations and entities that share or display SSNs to the general public and entities redact all but the last four digits of the SSN (expressed in his S. 1691, profiled in this month's Legislative Update). Currently, identity thieves gain access to SSNs by "shopping" around to find organizations that list the first five digits of the SSN and others that list the last four of the same number, therefore obtaining the entire nine digit number. The last four digits of SSNs are generated randomly, making them harder to link back to account holders.

Two other witnesses, **Rep. Ed Markey** (D-MA) and **Rep. Joe Barton** (R-TX), said that the SSN is a key to undue risks to individual consumers, and should be devalued. Both Congressmen are sponsors of the Social Security Number Protection Act (H.R. 968, profiled in the July Legislative Update), legislation that would make it a crime to buy or sell a Social Security number for commercial purposes (circumstances which exclude most survey and opinion research). Subcommittee **Chairman Michael McNulty** (D-NY) discussed his own proposal (H.R. 3046, mentioned in this month's Legislative Update) in hopes of melding it with H.R. 968.

The second panel consisted of witnesses from government agencies:

- **Social Security Administration (SSA)** - Inspector General Patrick O'Carroll testified that his agency is careful in issuing SSNs, but that the SSA lacks control over the useage of SSNs once they are issued. He compared how the college system has moved away from using SSNs, whereas K-12 schools have been caught recently exposing SSNs in public spaces.
- **Federal Trade Commission (FTC)** - Director Joel Winston of the Division of Privacy and Information Protection explained that, although the FTC cannot currently police the use of SSNs in the public space, his agency is working on new ways to authenticate individuals applying for SSNs. These new authenticating techniques will take some time to test and implement, he said. Most disturbingly, Winston reported that agency staffers were able to find the Social Security numbers and other financial information for about 10 people in 10 different places in just under an hour.
- **Government Accountability Office (GAO)** - Associate Director of Education, Workforce and Income Security, Dan Bertoni, explained that there is a problem of public disclosure, and solutions are hard to come by. He suggested that the Subcommittee should pass legislation to help agencies punish identity theft criminals. Winston concurred with Bertoni that the FTC cannot enforce the use of SSNs in the public space.

Warning to the Research Profession on SSNs
Probably the most important point to take away from this article, is that accessing SSNs is a risky proposition, even for experienced handlers of SSN data. Researchers should only undertake research involving SSNs in only limited and necessary circumstances. Any such information collected or handled should be managed only with consent from the individual and with appropriate security safeguards. This will not only promote data security, it will also help protect the profession from undue government regulation.

CMOR's Role
CMOR will continue to work on all aspects of identity theft, including the use and abuse of social security numbers, in order to protect the public and the research profession. For more information on privacy issues, please see the CMOR website or contact Howard Fienberg at hfienberg@cmor.org.

Disclaimer: The information provided in this message is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. CMOR advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

"Shielding the Profession"