Congress Considers Data Security Legislation

September 6, 2005

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

If nothing else positive has come from the seemingly unending string of data security breaches at corporations, universities and government agencies over the past year, they have, at the very least, illustrated the need for Congress to establish stronger protections for citizens' sensitive personal information.

(1) Congress Considers Data Security Legislation

If nothing else positive has come from the seemingly unending string of data security breaches at corporations, universities and government agencies over the past year, they have, at the very least, illustrated the need for Congress to establish stronger protections for citizens' sensitive personal information.

Data compromises at ChoicePoint, LexisNexis, the U.S. Air Force and other high-profile companies and organizations have heightened public concerns about loss of privacy and personal information. Federal and state lawmakers have responded to those concerns by proposing new legal protections specifically designed to protect citizens against the adverse effects of data security failures.

As a starting point, it must be recognized that there is still a need for baseline federal legislation to address the panoply of privacy issues posed by the digital revolution. Maintaining strong security is only one of a number of obligations that should apply to those who collect, use and store personally identifiable information. However, it is unlikely that current legislative efforts will address the larger issues of consumer privacy in the digital age, since enacting federal legislation on the full range of privacy concerns will require a longer and more inclusive dialogue than is currently underway.

Nonetheless, CDT believes there are a number of security issues, going beyond simply notifying citizens when their privacy has been compromised, that merit immediate attention. They share a common theme, arising from the rapid growth of the information services industry, the steep escalation in identity theft, and the government's increasing use of commercial data. These issues have been the subject of hearings and are addressed in one form or another in multiple pending bills.

CDT believes that any data privacy and security legislation that emerges from this Congress must represent a meaningful step forward, from a consumer perspective, over what states are already doing. CDT would oppose legislation that addressed the recent spate of data security breaches in an unduly narrow manner or in a way that resulted in consumers having weaker protections than those afforded under current state laws.

CDT's April 13, 2005 congressional testimony on securing electronic personal data: http://www.cdt.org/testimony/20050413dempsey.pdf [1]

CDT's March 2005 Policy Post on information security breaches:

http://www.cdt.org/publications/policyposts/2005/6 [2]

(2) CDT Recommends Key Elements of Legislation

In CDT's view, federal data security legislation should include the following elements:

- Notice of Breach: Entities, including government entities, holding sensitive personal data should be required to notify individuals in the event of a security breach. The notice of breach provision should afford at least as much protection as the California notice of breach law, while avoiding over-notification.
- Security Safeguards: Because notice would be given only after a breach had occurred, Congress should require entities that electronically store personal information to implement security safeguards, similar to those required by FTC rules under Gramm-Leach-Bliley (GLB) and California law. Civil fines should be available against companies that fail to comply with their own safeguards programs.
- Government Uses of Commercial Data: Congress should address issues raised by the federal government's growing use of commercial databases, especially in the law enforcement and national security contexts, by requiring public disclosure of the databases to which the government subscribes, government scrutiny of these databases' security safeguards as part of the contracting process, and measures to ensure data quality and redress when decisions about individuals are made on the basis of commercial data.
- Credit Report Freeze: Currently, consumers have limited options to protect themselves from fraud when they are notified of a breach or otherwise have concerns about the use of their data. Congress should allow customers to request a security freeze on their credit reports, as at least 10 states already have done.
- Social Security Number (SSN) Protection: SSNs have become the de facto national identifier and, especially when used as an authenticator, are key enablers of identity theft. Congress should seek to end the use of the SSN as an authenticator and should impose tighter controls on the disclosure, use, and sale of SSNs, with an appropriate phase-in period.
- Consumer Access to Data: Enabling individuals to access their personal data files is an important safeguard against inaccuracy and misuse, particularly when personal data is collected and maintained for disclosure to third parties for their use in risk assessment or other decision making. An access regime is well established under the Fair Credit Reporting Act (FCRA). Data security legislation should impose similar access requirements on information services companies that aggregate and sell personal data.
- Carefully Crafted Preemption: Nationwide notice of breach legislation should preempt individual state breach notification requirements, provided it affords at least as much protection as California's notification law. Federal legislation also should preempt inconsistent state legislation on other specific subjects addressed in the federal law (for example, security standards), following the model of GLB. Federal legislation should not, however, take the unusual step of preempting state common law or general consumer protection law.

(3) The Current Legislative Landscape

There are a number of bill in Congress in various stages of evolution that address some of the key elements listed above. Although several Senate and House committees have competing jurisdiction over these issues, three bills have emerged with bipartisan support from members of key committees. Given the public pressure to improve data security protections, these measures could come up this fall, even though lawmakers will be primarily focused on hurricane response efforts and Supreme Court nominations.

The Senate Commerce Committee has considered and approved a bill (S. 1408), introduced by Senators Smith (R-OR), Stevens (R-AK), Inouye (D-HI), McCain (R-AZ), Nelson (D-FL), and Pryor (D-AR), that provides for notice of breach, security safeguards, social security number protections,

and a security freeze. While some of the provisions in the Senate Commerce Committee bill provide good consumer protections, in CDT's view the preemption provision goes too far. It is drafted so broadly that it might preclude common law causes of action (cases alleging simple negligence, for example) under state law.

Prominent members of the Senate Judiciary Committee and House Energy and Commerce Committee are also working on bills, although neither committee has held a markup. The Senate Judiciary Committee bill (S. 1332), introduced by Committee Chairman Specter (R-PA) and Senator Leahy (D-VT), includes provisions on notice of breach, security safeguards, government use of commercial data, social security number protections, and consumer access to data.

Top members of the House Energy and Commerce Committee have circulated a draft bill that covers notice of breach, security safeguards, and consumer access to data. Lawmakers are likely to introduce the bill in September.

Other committees with potential claims of jurisdiction over some of these issues include the Senate Banking, House Financial Services, Senate Finance, and House Ways and Means. These committees could take up such issues as credit report freeze requirements or social security number protection.

Senate Commerce Committee bill, S. 1408: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01408: [3]

Specter-Leahy bill, S. 1332: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01332: [4]

Other bills pending in Congress can be found at http://www.cdt.org/legislation/109/3 [5]

Source URL: https://cdt.org/policy/congress-considers-data-security-legislation

Links:
[1] https://cdt.org/testimony/20050413dempsey.pdf
[2] https://cdt.org/publications/policyposts/2005/6
[3] http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01408:
[4] http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01332:
[5] https://cdt.org/legislation/109/3