CDT Recommendations:
Key Elements of Data Security Legislation
January 2007

In recent years, security breaches at corporations, universities and government agencies have heightened the public's concern about loss of control over sensitive personal information and have prompted policymakers at the state and federal level to propose legal protections. As a starting point, it must be recognized that there is still a need for baseline federal legislation to address the range of privacy issues posed by the digital revolution. Security is only one aspect of the custodial obligations that should apply to those who collect, use and store personally identifiable information. Trust and fairness in the information economy will not be fully established until a broad range of privacy issues has been addressed. However, enacting federal legislation on the full range of privacy issues will require a sustained and inclusive dialogue, so current legislative efforts are likely to take a narrower focus.

In this memo, we outline a constellation of security issues, going beyond breach notification, 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. Because these issues already have been the subject of hearings and multiple proposed bills, it would seem possible to achieve consensus among privacy advocates and data custodians. 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 have to oppose legislation that addressed the ongoing parade 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 and pending state laws.

In particular, federal legislation should include the following elements:

1. **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 protection that is at least as effective as what is already available under state statutes in California and elsewhere, while avoiding overnotification. A sensible approach could include a "two-tier" trigger requiring (i) notification to individuals unless there is no material risk of the data being misused, and (ii) simple notification to a government entity of any breach for which notification to individuals is judged unnecessary.

2. **Security Safeguards:** Because notice only kicks in after a breach has 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 security safeguards requirements.

3. **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. Provisions in S. 1789 from the 109th Congress provide an excellent model.

4. **Credit Report Freeze:** Currently, consumers in some states may 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 half the states already have done.

5. **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.

6. **Consumer Access to Data:** When personal data is collected and maintained for disclosure to third parties for their use in risk assessment or other decisionmaking, enabling individuals to access their personal data files is an important safeguard against inaccuracy and misuse. 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.

7. **Carefully Crafted Preemption:** Nationwide notice of breach legislation should preempt individual state breach notification requirements, provided it affords protection that is at least as effective as laws enacted in California and other states. 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.

For further information, please contact:
David Sohn, dsohn@cdt.org
202-637-9800