Restrictive Data Security Bill Advances in U.S. Senate

Howard Fienberg, MRA Director of Government Affairs

MRA E-news, October 2009, Volume 2

On November 5, 2009, the Senate Judiciary Committee passed a comprehensive data security and security breach notification bill: the Personal Data Privacy and Security Act (**S. 1490**), sponsored by Chairman Patrick Leahy (D-VT). **The Good**: S. 1490 would pre-empt most state data privacy and security program laws (like Massachusetts' and Nevada's) and all the state laws on breach notification. **The Bad**: The bill defines "sensitive personal information" and data security breach quite broadly.

The Committee rejected an amendment (13-6) from Ranking Member Jeff Sessions (R-AL) that would have limited the definition of breaches to exposures posing a significant risk of identity theft. Sessions said that the bill places "confusing burdens" on companies and organizations, often for "no real benefit".

S. 1490 now awaits consideration by the whole Senate.

Enhanced penalties

The Act would enhance the punishments and sentencing guidelines for identity theft and other violations of data privacy and security. For instance, anyone who "intentionally and willfully conceals the fact of …security breach and which breach causes economic damage to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both."

Who must implement a data privacy and security program?

According to Sections 301 and 302 of the Act, any company or organization "engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program …for protecting sensitive personally identifiable information." These provisions would not apply to any entity already subject to the data security requirements and enforcement of the Gramm Leach Bliley Act or HIPAA, nor to any public records "not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a news report or periodical."

The Act would also establish a safe harbor, whereby any entity would be deemed in compliance if it "complies with or provides protection equal to industry standards or

widely accepted as an effective industry practice, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information involved in the ordinary course of business of such business entity."

This data privacy and security program would have to be in place one year following enactment of S. 1490 into law.

On the plus side, S. 1490 would **pre-empt any state laws** from application to any entity subject to Sections 301 and 302, "with respect to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information."

What would be required of this data privacy and security program?

Sections 301 and 302 of the Act would require entities to "implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the … entity and the nature and scope of its activities."

The program would have to be designed to:

a. use "**encryption**";
b. ensure the privacy, security, and confidentiality of sensitive personally identifying information;
c. protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and
d. protect against unauthorized access to use of sensitive personally identifying information that could create a significant risk of harm or fraud to any individual.

The program would also be subject to intensive risk assessment, management, testing and control.

Moreover, S. 1490 would require such an entity to regularly "monitor, evaluate, and adjust, as appropriate" its program "in light of any relevant changes in--

1. technology;
2. the sensitivity of personally identifiable information;
3. internal or external threats to personally identifiable information; and
4. the changing business arrangements of the … entity, such as--
    a. mergers and acquisitions;
    b. alliances and joint ventures;
    c. outsourcing arrangements;
    d. bankruptcy; and
    e. changes to sensitive personally identifiable information systems.

Relations with service providers

If the entity works with service providers who are not subject to these requirements, the entity would have to "exercise appropriate due diligence in selecting those service

providers for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue." More importantly, like HIPAA covered entities have to do with business associates, the entity would have to "require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements" of Sections 301 and 302.

Violations of Sections 301 and 302

Violators of these sections would be subject to "civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation." Any "intentional or willful violation" would be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation. The FTC would have enforcement authority for these sections.

These sections could also be enforced by civil actions by a state Attorney General, or any state or local law enforcement agency authorized by a state Attorney General or by State statute to prosecute violations of consumer protection law.

Security breach notifications

S. 1490 would require that any entity "that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired." In general, the obligation for notification applies to whoever owns or licenses the information – entities subject to a breach that don't own or license the information breached are required to notify the owner or licensor.

Notifications would be required "without unreasonable delay following the discovery" of a breach. "Reasonable delay" would include "any time necessary to determine the scope of the security breach, prevent further disclosures, and restore the reasonable integrity of the data system and provide notice to law enforcement when required."

In addition to notifying affected U.S. residents, entities would have to inform the Secret Service if: (1) the number of individuals subject to a breach exceeds 10,000; (2) the breach involves "a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide"; (3) the breach involves databases owned by the Federal Government; or (4) the breach involves primarily sensitive personally identifiable information of known Federal employees or contractors involved in national security or law enforcement.

Exemption from notification requirements

Entities would be exempt from notice requirements if

1. a risk assessment concludes that—
    a. there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the encryption of such information establishing a presumption that no significant risk exists; or
    b. there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the rendering of such sensitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, establishing a presumption that no significant risk exists;
2. without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the Secret Service, the entity notifies the Secret Service, in writing, of--
    a. the results of the risk assessment; and
    b. its decision to invoke the risk assessment exemption; and
3. the Secret Service does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

Enforcement of notification requirements

Under S. 1490, the Attorney General enforces the notification requirements and could levy a civil penalty of not more than $1,000 per day per individual whose sensitive personally identifiable information was breached, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional. State attorneys general are similarly empowered to bring civil actions.

S. 1490 would **pre-empt all state breach notification laws**, except for certain state requirements for including information regarding victim protection assistance.

Definitions

Sen. Leahy would define "**encryption**" to mean "the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by a widely accepted standards setting body or, has been widely accepted as an effective industry practice which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data" and "includes appropriate management and safeguards of such cryptographic keys." (Encryption was the focus of last month's e-news article, "Nevada Mandates Encryption Standard")

"**Security breach**" would be defined as "compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there

is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization and which present a significant risk of harm or fraud to any individual." This definition excludes: "(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure; or (ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements."

S. 1490 would define the term "**sensitive personally identifiable information**" as "any information or compilation of information, in electronic or digital form that includes either (A) or (B):

(A) an individual's first and last name or first initial and last name in combination with any one of the following data elements:
(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.
(ii) Any 2 of the following:
(I) Home address or telephone number.
(II) Mother's maiden name, if identified as such.
(III) Month, day, and year of birth.
(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.
(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(B) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

Conclusion

S. 1490 is one of multiple bills snaking their way through Congress which address data security and breach notification. Our biggest concerns with S. 1490, as with other bills, are (1) a more careful distinction between "sensitive personally identifiable information" and more mundane data, and (2) pre-emption of all the conflicting state laws. CMOR will continue to work with the relevant committees and staff to see that whatever data security legislation becomes law reflects our top concerns for the research profession.