Bloomberg Law Reports®

October 17, 2011

Technology Law

Privacy & Information Law

Proposed Federal Cybersecurity Legislation: A New Landscape for Regulation of Data Security and Security Breach Notification




Contributed by Marcus A. Asner, Nancy L. Perkins, Ronald D. Lee, and James D. Flynn, Arnold & Porter LLP

Recent high-profile data security breaches at the IMF, Pentagon and U.S. Senate, and companies like Google, Sony and RSA–to name a few–have elevated concerns about vulnerabilities in the nation's cybersecurity in both the public and private sectors. According to the White House Office of Management and Budget, "[t]he dramatic increase in cyber crime and the repeated cyber intrusions into critical infrastructure demonstrate the need for improved security."[1] President Barack Obama has described the cyber threat as "one of the most serious economic and national security challenges we face as a nation."[2]

In May, the Obama Administration sent a proposal to Congress designed to lay the foundation for comprehensive cybersecurity legislation.[3] In response to the Administration's proposal and recent high-profile cyber attacks, members of both the House and the Senate have introduced a number of bills drafted to address various aspects of the cybersecurity issue. In addition, House Speaker John Boehner (R-OH) has appointed Representative Mac Thornberry (R-TX) to oversee an exclusively Republican task force to review and report on the President's proposal, and Senate Majority Leader Harry Reid (D-NV) and Minority Leader Mitch McConnell (R-KY) are working together on a comprehensive cybersecurity legislative package.

This article focuses on three of the more recent legislative proposals that would, among other things, require covered business entities to develop and implement data privacy and security programs, notify individuals whose "sensitive personally identifiable information" (SPII) has been compromised, and impose criminal penalties for individuals who intentionally conceal the fact that a data breach has occurred. With certain exceptions, all three bills would preempt state laws requiring notification of data security breaches–a welcome relief from the current patchwork of state security breach notification laws. It appears that some form of these proposals almost certainly will become federal law, and affected businesses should consider now the potential impact of and implications for their future practices involving SPII.

Proposed Data Security and Security Breach Notification Legislation

– Overview

On September 22, 2011, the Senate Judiciary Committee voted to report three amended data security bills to the Senate.[4] The "Personal Data Privacy and Security Act of 2011" (S. 1151),

introduced by Committee Chairman Patrick Leahy (D-VT), would require covered business entities to develop comprehensive data privacy and security programs, notify individuals whose SPII has been compromised, and impose criminal penalties for individuals who intentionally conceal the fact that a data breach has occurred. The "Data Breach Notification Act of 2011" (S. 1408), introduced by Senator Dianne Feinstein (D-CA), is a narrower version of the Leahy bill that would mandate breach notification and criminalize concealment of a data breach, but would not require the development of data privacy and security programs. The "Personal Data Protection and Breach Accountability Act of 2011" (S. 1535), sponsored by Senator Richard Blumenthal (D-CT), is a somewhat broader version of Chairman Leahy's measure.

Each of the bills defines a "security breach" generally as a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or that there is a reasonable basis to conclude has resulted in, the unauthorized access of SPII, or access of SPII in excess of authorization.[5] The definition of SPII under each of the bills is broad and includes such information as, among other things, an individual's first initial and last name, in combination with any two of a home address, telephone number, birthdate or mother's maiden name; a non-truncated social security or government-issued identification number; biometric data such as finger or voice print; or a financial account number.[6]

– The Leahy Bill

The Leahy bill's requirements for data privacy and security programs generally would apply to any "business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of [SPII] in electronic or digital form on 10,000 or more United States persons."[7] The bill specifically exempts several categories of businesses from its requirements, however:

- Financial institutions subject to the data security requirements and implementing regulations of the Gramm-Leach-Bliley Act (GLBA), and subject to examinations for compliance by a federal functional regulator or state insurance authority, or subject to compliance with part 314 of title 16 of the Code of Federal Regulations ("Standards for safeguarding customer information");[8]
- Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as defined in HIPAA and its implementing regulations;
- Business entities acting as a business associate under and in compliance with HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act[9] and regulations promulgated thereunder; and
- Service providers for any electronic communication by a third party, to the extent the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.[10]

The data privacy and security program provisions of the Leahy bill would preempt state law "with respect to administrative, technical, and physical safeguards for the protection of personal information,"[11] except any state regulations implementing the GLBA.[12]

With respect to the data breach notification requirements, the Leahy bill would require that any "agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects [SPII] shall, following the discovery of a security breach of such information, notify any resident of the United States whose [SPII] has been, or is reasonably believed to have been, accessed, or acquired."[13] Recognizing that such requirements already apply to entities subject to the GLBA, HIPAA, and the HITECH Act, the Leahy bill would exempt these entities–including HIPAA business associates and vendors of personal health records (PHRs) and their service providers.[14]

The bill's data breach notification provisions would preempt "any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or any agency of a security breach," except that a state could require that the notice also include information regarding victim protection assistance provided for by that state.[15]

– The Feinstein Bill

The Feinstein bill largely mirrors the Leahy bill, although its scope is limited to data security breach notification requirements. It too would preempt state security breach notification mandates and would exempt financial institutions regulated by federal functional regulators under the GLBA.[16] The Feinstein bill also makes plain that its requirements are not meant to supersede the data privacy and security requirements of the GLBA or the HITECH Act.[17]

– The Blumenthal Bill

The Blumenthal bill also is very similar to the Leahy bill: it includes both data security protection program requirements and security breach notification requirements, and also provides exemptions for entities regulated by the GLBA, HIPAA, and the HITECH Act.[18] However, the Blumenthal bill, although it would preempt state requirements for data security *breach notifications*,[19] would *not preempt* state law with respect to data security *protection programs* (other than through general principles of conflict preemption).

Implications of Proposed Legislation

– Data Privacy and Security Programs

Few states have enacted laws that require business entities, other than financial institutions, to develop and implement data privacy and security programs, so the enactment of such a requirement at the federal level would be a significant development in this area of the law.

The Leahy and Blumenthal bills would require covered business entities to create a data privacy and security program designed to ensure the privacy, security, and confidentiality of SPII; protect against any anticipated vulnerabilities to the privacy, security, or integrity of SPII; and protect against unauthorized access to use of SPII that could create a significant risk of harm or fraud to any individual.[20] To achieve these objectives, a covered entity would be required to: (1) regularly assess, manage and control risks to improve its data privacy and security program; (2) provide employee training to implement its program; (3) conduct tests to identify security vulnerabilities; (4) ensure that overseas service providers, not otherwise subject to the proposed Act but retained by covered business entities to manage SPII, take reasonable measures to secure data; and (5) periodically assess the program to ensure that it addresses current threats.[21]

The Leahy bill would give authority to the FTC to bring an enforcement action for any violations.[22] Senator Blumenthal's bill would vest such authority with the U.S. Attorney General.[23] Under the Leahy bill, business entities that violate the data privacy and security program provisions would be subject to a civil penalty of $5,000 per violation, per day, up to a maximum of $500,000 per violation;[24] Senator Blumenthal's bill would cap penalties for non-willful violations at $20 million per violation.[25] Both would double penalties for willful violations.[26] The Leahy and Blumenthal bills would also give states the right to bring civil actions on behalf of their residents.[27] While the Leahy bill would not create a private cause of action for violations, significantly, the Blumenthal bill would expressly create a private right of action to allow individuals to seek up to $20 million in damages for violations of the data privacy and security program provisions.[28]

– Security Breach Notification

Most states have enacted laws that require companies to notify their customers that the security of the customers' SPII has been compromised. However, the state laws differ from one another in numerous respects, and keeping track of their details, and attempting to comply with all applicable requirements, has been a major headache for businesses that handle SPII. Thus, the preemption of state law provided by the Senators' bills would be a much-welcomed relief from the costs associated with complying with a patchwork of nuanced state requirements.

Each of the three federal bills would require covered business entities to "notify any resident of the United States whose [SPII] has been, or is reasonably believed to have been, accessed, or acquired."[29] Each bill also would require businesses that do not own or license the compromised information to notify the owner or licensee, who then would be required to make the proscribed notification.[30] In some circumstances, covered business entities would also be required to notify credit-reporting agencies and law enforcement authorities.[31]

Under each bill, notifications must be made "without unreasonable delay."[32] Under the Leahy and Feinstein bills, such delay cannot exceed 60 days.[33] Notification will still be timely, however, if the FTC determines that additional time is warranted under a multi-factor test, or, in some cases, unnecessary, if a federal law enforcement agency determines that notification would impede a criminal investigation or national security, or if the business entity participates in a financial fraud prevention program.[34] Notification must be made personally by mail, telephone or email, and, in addition, must be made by "media notice" if the number of affected individuals in any one state exceeds 5,000.[35] The content of the notification must include a description of the SPII at risk, several toll-free contact numbers, and, under the Leahy and Blumenthal bills, the name of the business entity that has a direct business relationship with the individual whose SPII was compromised.[36]

Not every breach will trigger the notification requirement, however. Each bill contains an important safe harbor where a risk assessment conducted by the business entity concludes that there is "no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to the individuals whose [SPII] was subject to the security breach."[37] Notably, each bill would establish a presumption that no significant risk exists where SPII is encrypted or otherwise rendered "unusable, unreadable or indecipherable."[38] The Leahy and Blumenthal bills also set forth the requirements for such a risk assessment.[39]

The Leahy and Blumenthal bills would provide for enforcement of the notification requirements by the Attorney General of the United States, or the FTC as an unfair or deceptive act or practice.[40] Violators of the Leahy bill would be subject to a civil penalty of $11,000 per day, "per incident whose personal information [sic] was, or is reasonably believed to have been, accessed or acquired by an unauthorized person."[41] Senator Feinstein's bill would provide for a civil penalty of "$11,000 per day per security breach," but would cap damages for a failure to comply with the provisions of her bill at $1,000,000, except that willful or intentional violators would be subject to double the maximum penalty.[42] Senator Blumenthal's bill would provide for a civil penalty of $500 per day, per individual whose SPII was compromised, up to $20 million per violation of the notification provisions, unless the violation is willful.[43] In some circumstances, State attorneys general also could bring civil actions seeking injunctive relief and civil penalties for any violation.[44] The Leahy and Feinstein bills expressly disclaim a private cause of action for a violation of the bill's notification requirements.[45] The Blumenthal bill, in contrast, would expressly create a private

right of action to allow individuals to seek up to $20 million in damages for violations of the data privacy and security program provisions.[46]

All three bills also would make it a criminal offense to intentionally and willfully conceal the fact that a security breach has occurred.[47] Criminal liability would attach under the Leahy and Feinstein bills where the defendant had knowledge of the breach, was aware that notice was required under the applicable provisions of the bill, and the breach resulted in economic harm of $1,000 or more to any person.[48] Senator Blumenthal's bill would require only some resulting economic harm or "substantial emotional distress" to one or more persons.[49] Willful concealment under the bills would be punishable by fines and up to five years imprisonment.[50]

Each of the three legislative proposals reported on September 22 would, if enacted, result in a number of significant changes to an already complex legal environment. Arnold & Porter will be monitoring the landscape for developments as they occur and can be contacted for updates.

Marcus A. Asner is a partner of Arnold & Porter LLP in New York. Previously, he served as an Assistant United States Attorney for the Southern District of New York, where he was the Chief of the Major Crimes and Computer Hacking/Intellectual Property Unit for two years, and served as the Identity Theft coordinator for the Southern District of New York. He may be reached at Marcus.Asner@aporter.com or 212.715.1789.

Nancy L. Perkins is counsel of Arnold & Porter LLP in Washington, D.C. Ms. Perkins regularly advises clients on federal and state requirements for privacy and security of medical, financial, and electronic data. Ms. Perkins can be reached at Nancy.Perkins@aporter.com or 202.942.5065.

Ronald D. Lee is a partner of Arnold & Porter LLP in Washington, D.C. He was formerly General Counsel of the U.S. National Security Agency and Associate Deputy Attorney General with the U.S. Department of Justice, handling national security, cyber and counterterrorism matters. Mr. Lee can be reached at Ronald.Lee@aporter.com or 202.942.5380.

James D. Flynn is an associate of Arnold & Porter LLP in New York and a member of the litigation, securities enforcement and litigation, and white collar criminal defense practice groups. Mr. Flynn's practice focuses on general and complex commercial, intellectual property, and securities litigation, and corporate internal investigative matters. He may be reached at James.Flynn@aporter.com or 212.715.1792.

[1] *See* Letter from Jacob Lew, Director, Office of Management and Budget, to Hon. John Boehner, Speaker, House of Representatives and Hon. Joseph R. Biden, President, Senate (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-letters-to-congress-house-signed.pdf (last visited Oct. 3, 2011).

[2] *Id.*

[3] *See id.*

[4] The text of the three bills, and several proposed amendments to those bills, is available on the Senate Committee on the Judiciary's website at http://judiciary.senate.gov/legislation/BusinessMeetingResults.cfm (last visited Oct. 3, 2011).

[5] *See* S. 1151, 112th Cong. § 3(a)(11) (2011); S. 1408, 112th Cong. § 14(8) (2011); S. 1535, 112th Cong. § 3(a)(15) (2011)

[6] *See* S. 1151, § 3(a)(12); S. 1408, § 14(7); S. 1535, § 3(a)(13). The Leahy and Blumenthal bills would grant the Federal Trade Commission (FTC) authority to modify the definition of SPII by rulemaking. *See* S. 1151, § 3(b); S. 1535, § 3(b).

[7] S. 1151, § 201(b).

[8] A proposed amendment to the Leahy bill (ALB11713) would simplify this provision by stating that financial institutions subject to regulation under the GLBA, and the jurisdiction of an agency or authority described in section 501(b) of the GLBA, would be exempt.

[9] Specifically, the bill would exempt business entities subject to, and currently in compliance with, the privacy and data security requirements of sections 13401 and 13404A of division A of the American Reinvestment and Recovery Act of 2009. *Id.* § 201(c)(2)(B)(ii).

[10] *Id.* § 201(c).

[11] *Id.* § 204(a).

[12] *Id.* § 204(b).

[13] *Id.* § 211(a).

[14] *Id.* § 211(e).

[15] *Id.* §§ 219, 214(b). A proposed amendment to the Leahy bill (ALB11713) would clarify that nothing therein would operate to modify, limit or supersede the operation of the GLBA, HIPAA or the HITECH Act.

[16] S. 1408, §§ 3(d), 11(a).

[17] *Id.* § 11(b).

[18] S. 1535, §§ 201(c), 212(d).

[19] *Id.* § 221(a).

[20] S. 1151, § 202(a)(2); S. 1535, § 202(a)(2).

[21] S. 1151, § 202(a)-(e); S. 1535, § 202(a)-(e). Among other things, the bills would require that covered non-exempt business entities take measures to protect SPII "during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means . . . ." S. 1151, § 202(a)(4)(B)(iii); S. 1535, § 202(a)(4)(B)(iii);

[22] S. 1151, § 203(b).

[23] S. 1535, § 203(a)(1).

[24] S. 1151, § 203(a)(1).

[25] S. 1535, § 203(a)(1).

[26] *See* S. 1535, § 203(a)(2); S. 1535, § 203(a)(2).

[27] S. 1151, § 203(c); S. 1535, § 204.

[28] *See* S. 1151, § 203(d); S. 1535, § 205.

[29] S. 1151, § 211(a); S. 1408, § 2(a); S. 1535, § 211(a).

[30] S. 1151, § 211(b)(2); S. 1408, § 2(b)(2); S. 1151, § 211(b)(2).

[31] S. 1151, §§ 215, 216; S. 1408, §§ 6, 7; S. 1535, §§ 216, 217.

[32] S. 1151, § 211(c)(1); S. 1408, § 2(c)(1); S. 1535, § 211(c)(1).

[33] S. 1151, § 211(c)(2)(B)(i); S. 1408, § 2(c)(2)(b)(i). Senator Blumenthal's bill does not specifically define "reasonable delay" as 60 days or less. *See* S. 1535, § 211(c).

[34] S. 1151, §§ 211(c)-(d), 212(a), 212(c); S. 1408, §§ 2(c)-(d), 3(a), 3(c); S. 1535, §§ 211(c)-(d), 212(a), 212(c).

[35] S. 1151, § 213; S. 1408, § 4; S. 1535, § 213.

[36] S. 1151, § 214; S. 1408, § 5; S. 1535, § 214. As noted above, states may also require additional content regarding victim protection assistance provided for in that state. S. 1151, § 214(b); S. 1408, § 5(b); S. 1535, § 214(b).

[37] S. 1151, § 212(b); S. 1408, § 3(b); S. 1535, § 212(b).

[38] *See* S. 1151, § 212(b)(2); S. 1408, § 3(b)(2); S. 1535, § 212(b).

[39] S. 1151, § 212(b)(3); S. 1535, § 212(b)(3).

[40] S. 1151, § 217; S. 1535, § 212(b)(3). Senator Feinstein's bill would not grant enforcement authority to the Federal Trade Commission. *See* S. 1408, § 8.

[41] S. 1151, § 217(b). A proposed amendment to the Leahy bill (ALB11713) would clarify that violators are subject to a civil penalty of $11,000 per day per security breach, not to exceed $1 million, with willful or intentional violators subject to an additional $1 million penalty.

[42] S. 1408, § 8(a), (b).

[43] S. 1535, § 218(a). The failure to conduct a risk assessment or to submit a misleading risk assessment in violation of section 212(b)(2)(C) is presumptively willful or intentional conduct under the Blumenthal bill. *See id.* § 218(a)(2).

[44] S. 1151, § 218; S. 1408, § 9; S. 1535, § 219.

[45] S. 1535, § 218(f); S. 1408, § 9(f).

[46] S. 1535, § 220. Blumenthal's bill also provides that that a covered business entity that is required to make a notification of a security breach "shallpay, upon request . . . any costs or damages incurred by the individual as a result of such security breach, including costs associated with identity theft . . . ." *Id.* § 215(c).

[47] S. 1151, § 102; S. 1408, § 10; S. 1535, § 101.

[48] S. 1151, § 102(a); S. 1408, § 10(a).

[49] *See* S. 1535, § 101.

[50] S. 1151, § 102(a); S. 1408, § 10(a); S. 1535, § 101(a).