Clients&FriendsMemo

The Obama Administration's Personal Data Notification & Protection Act: An Analysis

February 12, 2015

On January 12, 2015, President Obama proposed the Personal Data Notification & Protection Act, which would create a federal standard for data breach notification.[1] The proposed bill is part of a more wide-ranging effort by the Obama administration to shore up the nation's cybersecurity.[2] The measure comes at a time when both the public and private sectors, especially the retail and banking industries, have been under increasing attack by cyber criminals and state actors; the Sony hack attributed to North Korea is only the latest in a series of high-profile cyber incidents.

The Obama administration's draft bill follows a long line of legislative proposals that have failed to gain passage despite the rising incidence of high-profile data breaches. In just the last two years, five data breach notification bills were introduced in the Senate alone, yet none garnered sufficient support for passage.[3] However, the public's heightened interest in the issue, combined with the support of key business groups, might be enough to finally break the gridlock.

Business groups such as the National Retail Federation[4] support the Obama administration's proposed legislation because it creates a single breach notification standard. These groups—which are likely to have greater sway with Republicans and conservative Democrats—reason that

---

1 *See* The Personal Data Notification & Protection Act, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

2 This effort also includes legislation that would facilitate greater information sharing between the private sector and the federal government and, separately, update law enforcement provisions related to the prosecution of computer crime. *See* Updated Department of Homeland Security Cybersecurity Authority and Information Sharing Proposal, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf; Updated Law Enforcement Provisions Related to Computer Security, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

3 *See* Data Security Act of 2014, S. 1927, 113th Cong. (Sens. Carper & Blunt); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (Sen. Rockefeller); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (Sen. Leahy); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (Sen. Blumenthal); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (Sen. Toomey).

4 *See Retailers Renew Call for Federal Data Breach Notification Law*, NATIONAL RETAIL FEDERATION (Jan. 12, 2015), https://nrf.com/media/press-releases/retailers-renew-call-federal-data-breach-notification-law.

even a tougher federal standard would be simpler to comply with than the current patchwork of 47 different—and often conflicting—state laws.[5] Meanwhile, consumer protection groups are concerned because the federal legislation would preempt state data breach notification laws, including those that offer greater protection than the proposed federal standard.[6]

The proposed legislation's ultimate success likely will turn on whether both sides can reach agreement on a middle ground and recognize that neither businesses nor privacy advocates will be able to cherry-pick all of their favorite provisions from existing state laws and earlier federal proposals. The following is a brief analysis of the proposed bill's key provisions.

Defining Personal Information

The Obama administration's proposal would require businesses to notify individuals whose sensitive personally identifiable information ("SPII") has been or is reasonably believed to have been acquired or accessed without authorization unless there is no reasonable risk of harm or fraud to the individual. The bill defines SPII to include:

> (1) an individual's first and last name or first initial and last name in combination with any two of the following data elements:
>
> > (A) home address or telephone number;
> >
> > (B) Mother's maiden name;
> >
> > (C) month, day, and year of birth;
>
> (2) a non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number;
>
> (3) unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;
>
> (4) a unique account identifier, including a financial accounting number or credit or debit card number, electronic identification number, user name, or routing code;

---

[5] *See* Brendan Sasso, *Why Businesses Love Obama's Push for Security Regulation*, NATIONAL JOURNAL (Jan. 12, 2015), http://www.nationaljournal.com/tech/why-businesses-love-obama-s-push-for-security-regulation-20150112.

[6] *See* G.S. Hans, *White House Data Breach Legislation Must Be Augmented to Improve Consumer Protection*, CENTER FOR DEMOCRACY & TECHNOLOGY (January 16, 2015), https://cdt.org/blog/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.

(5) a user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account; or

(6) any combination of the following data elements:

(A) an individual's first and last name or first initial and last name;

(B) a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or

(C) any security code, access code, or password, or source code that could be used to generate such codes or passwords.

This definition is more expansive than that which is found in most of the earlier Senate proposals.[7] The Obama administration's proposal also authorizes the Federal Trade Commission ("FTC" or the "Commission") to use its rulemaking authority to amend the definition of SPII, thereby ensuring that the law will remain relevant as technology evolves, while also introducing some uncertainty about the scope of future breach notification obligations.

Identifying a Data Breach—The Trigger for Notification

The proposed legislation also details when a security breach gives rise to an obligation to notify affected individuals. The administration's proposal broadly defines "security breach" to include instances in which there is a reasonable basis to conclude that an unauthorized acquisition of or access to SPII occurred.[8] Individual notification generally is required when a security breach occurs, but a risk-based exemption narrows this obligation. Individual notification is not required where "there is no reasonable risk of harm or fraud" to the individual whose SPII was acquired or accessed. While relieving businesses of notification obligations in some cases, this exemption is not as broad as that which is found in many state laws and previous federal proposals. Many states, and several earlier federal proposals, require notification only in cases where substantial harm or a specific kind of harm—identity theft—is likely. The result is that the proposed legislation

---

[7] Senator Toomey's bill, for example, would have included only names, social security numbers, government identification numbers, and financial account numbers with required security codes. At the other end of the spectrum, the definition of "sensitive personally identifiable information" in Senator Blumenthal's bill included everything in the Obama proposal and added an individual's medical history.

[8] *See* § 1(g) ("The term 'security breach' means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in – (A) the unauthorized acquisition of sensitive personally identifiable information; or (B) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.").

likely will require individual notification more often than would be required under many existing state laws and previous legislative proposals.

The bill acknowledges the burden that notification can place on small businesses by requiring only those "businesses that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information about more than 10,000 individuals in any 12-month period" to notify individuals of a security breach that may affect their SPII.[9] The proposal also takes into consideration the expanding number of businesses that give vendors access to their SPII. For example, a retailer might contract with a vendor to maintain its point-of-sale terminals, thereby sharing the SPII found on those terminals with the vendor. The bill relieves vendors—and other business entities that do not own or license personally identifiable information—of any obligation to notify individuals of a breach of that information unless there is a contractual agreement to the contrary. Rather, vendors must notify the owners or licensees of SPII in the event of a security breach, and those owners and licensees in turn must provide any required notification.[10]

Risk Assessments—The Key to Avoiding Unnecessary Notification

As discussed above, the bill's core proposition is that, absent an exception, a business must notify customers of any security breach, regardless of whether that breach involves one individual's driver's license number or the credit files of millions of individuals. The broad reach of this general rule, however, is tempered by several exceptions. The principal exception allows businesses to avoid the individual notification requirement in instances where "there is no reasonable risk of harm or fraud" to the individual whose SPII was acquired or accessed.[11] The only way to make that determination and avoid the notice requirement is to conduct a post-breach risk assessment.

There is a narrow window for a business to conduct a risk assessment after it learns of a security breach. Within 30 days after discovering a security breach, a business must notify the FTC of the results of the risk assessment and the business's decision to invoke the risk assessment exemption.

The risk assessment must be conducted "in a reasonable manner or according to standards generally accepted by experts in the field of information security." The assessment must also

---

[9] At the same time, this provision would appear to require businesses to track at least monthly their use, access, transmission, disposal, or collection of SPII, so that in the case of a breach, they can determine whether the 10,000 number has been reached.

[10] The bill also provides limited exemptions to the individual notification requirement for breaches affecting credit card data and certain HIPAA-covered entities.

[11] The bill provides an even greater incentive for businesses to take a proactive approach to safeguarding personal information by creating a rebuttable presumption that no reasonable risk of harm exists when the information subject to a security breach is encrypted. *See* § 102(b)(1)(A) ("If the data at issue was rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security, there shall be a presumption that no reasonable risk exists.").

include, to the extent available, at least six months of data that logs every "communication or attempted communication with a database or data system containing sensitive personally identifiable information." The logs must contain "all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information." This data is more granular—and far more sensitive—than the information that any comparable state law or federal legislative proposal requires a business to turn over to the government.

When and How to Provide Notice

Under the proposal, businesses must make required notifications "without unreasonable delay," which shall not exceed 30 days unless the entity demonstrates to the FTC that additional time is necessary, or the government delays notification for the purposes of law enforcement or national security. Individual notice may be provided by mail, telephone, or e-mail (if the individual has consented to receive notice by e-mail). In addition, a business must provide notice to the media when the number of affected individuals in any one state exceeds 5,000. Notably absent is a provision in many state laws and earlier federal legislative proposals that allows for substitute notification through the media alone when individual contact information is not available or the cost of providing individual notice is excessive. The content of a notice, regardless of the method by which it is transmitted, must include a description of the categories of SPII acquired or accessed, a toll-free number that an individual can call to find out what types of SPII a company maintains about him or her, and contact information for the major credit reporting agencies and the FTC.[12]

Notifying the Government of a Data Breach

In addition to ensuring that individuals receive timely notice of security breaches that affect their SPII, the bill also obligates businesses to report security breaches to the federal government when certain criteria are met. Government notice may be required even if a risk assessment determines that no individual notification is required. The Secretary of Homeland Security is directed to designate the entity that will receive this information and disseminate it to the U.S. Secret Service, the FBI, and the FTC. The bill also sets the criteria that trigger the government reporting obligation. The obligation to report arises when the SPII of more than 5,000 individuals is accessed, the breach involves a database containing such information about more than 500,000 individuals, or the breach involves federal government databases or the SPII of individuals known to the business to be federal employees or contractors involved in national security or law enforcement. Notably, just as the FTC can use its rulemaking authority to change the definition of SPII, it can also

[12] In a provision favored by consumer advocates, the bill allows a state to require that a notice include additional information about the state's victim protection assistance. For example, California requires individual notice of a data breach to offer identity-theft prevention products. This is the only instance in which the administration's proposal does not preempt state data breach notification laws.

promulgate regulations to amend the thresholds for when government notice must be provided. The timeline for notifying the government is even more compressed than for individual notification, with government notice being required at least 72 hours before individual notice, or 10 days after discovery of the security breach—whichever comes first.

Enforcement by the FTC and State Attorneys General

The proposal provides for enforcement of the bill's breach notification requirements at both the federal and state level. At the federal level, compliance is enforced by the FTC under the Federal Trade Commission Act ("FTCA"). Any violation of the bill is defined to be an unfair or deceptive trade practice that is subject to the jurisdiction of the Commission, even if the business entity does not meet the other jurisdictional requirements under the FTCA.[13]

In addition to enforcement by the FTC, state attorneys general are empowered to bring civil actions seeking injunctive relief or civil penalties of up to $1,000 per day for each individual whose SPII was compromised—up to $1 million per violation. However, there is no cap on the civil penalties that state attorneys general can recover when the business entity is found to have acted willfully or intentionally. Before filing an action, a state must provide written notice to the Attorney General and the FTC, which in turn may move to stay the action, intervene in the action, initiate its own action, or file petitions for appeal. Once the Commission institutes an action, state attorneys general cannot file subsequent parallel actions. The proposal does not include a private right of action.

Conclusion

There is mounting pressure on the federal government to do more to protect Americans from cyber attacks and computer crime. However, the success of the Obama administration's proposal is not a foregone conclusion, especially if consumer protection groups advocate strongly against a law that preempts what they believe are stronger consumer protections included in some existing state laws. Agreeing on the details will be challenging for Congress, but the growing consensus that a national standard is needed makes this one of the more promising areas in which the new Congress could make real progress.

In the midst of this debate over the need for a national data breach notification law, businesses must keep the bigger cybersecurity picture in mind. Indeed, businesses do not need to wait for

[13] For example, under the FTCA, the FTC does not have jurisdiction over specific types of entities such as banks, credit unions, and certain nonprofit organizations. However, the proposed bill would allow the FTC to regulate even those entities' compliance with the federal breach notification standard. Despite this broad enforcement authority, a handful of checks limit the Commission's investigative power. The Commission must consult with the Attorney General before beginning an investigation, and in certain instances, must coordinate its investigations with the Federal Communications Commission or the Consumer Financial Protection Bureau.

legislation before implementing the most critical aspects of an effective cybersecurity strategy. Minimizing the occurrence and severity of cyber attacks and data breaches fundamentally depends on creating a corporate culture in which individual users, from line workers to chief executives, exercise discipline in how they use technology every time they log on.[14] Legislation alone cannot promote good information security hygiene. More than any other area of business risk, cybersecurity requires a proactive approach that focuses not only on compliance with existing laws and regulations, but also on implementing and continuously refining best practices and technological solutions to address an ever-evolving threat.

* * * *

Please feel free to contact any of the following Cadwalader lawyers if you have any questions about this Clients & Friends Memo.

Kenneth L. Wainstein	+1 202 862 2474	ken.wainstein@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com
Peter Carey	+1 202 862 2339	peter.carey@cwt.com

[14] *See generally* PONEMON INST. LLC, 2015 STATE OF THE ENDPOINT REPORT: USER-CENTRIC RISK 1 (2015), *available at* http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf ("The biggest problem identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office.").