THE
NATIONAL LAW REVIEW

President Obama's Security Breach Notification Bill Needs Work

Article By
Data Privacy & Information Security
Poyner Spruill LLP
p.s. publications full of ideas

- Consumer Protection
- Communications, Media & Internet

- All Federal

Friday, January 16, 2015

The White House recently released The Personal Data Notification & Protection Act as part of an extensive proposal to safeguard data and improve cyber security. The proposal was released in a preview of the State of the Union address and comes close on the heels of Sony's (second) epic breach, attributed by most to hackers associated with North Korea. Many privacy and data security professionals have hoped for years to see a federal breach notification bill succeed, even a tough one, because one tough federal law seems like a good trade-off for a sorely-needed uniform breach notification rule. With more than 50 breach laws in play across the states and U.S. territories, breach notice has become a largely-unproductive slog through disparate and sometimes contradictory requirements. So to you, the optimistic reader who felt your heart warm at the prospect of renewed federal interest in cleaning up the states' mess, we direct this alert full of practical observations about the content of President Obama's proposal. Observation #1: Perhaps a more apt title for the Act is "The Be Careful What You Wish For Act."

Low Risk, Mistaken Access May Be a Security Breach

Like many state breach laws, the proposal would treat as a security breach any unauthorized acquisition of or access to "*sensitive personally identifiable information*" (SPII) that compromises the security, confidentiality, or integrity of that SPII. Unlike

many state corollaries, however, the proposal's security breach definition lacks an exception for employees or agents who access SPII mistakenly but in good faith, albeit without authorization. Although this common type of unauthorized access arguably does not "compromise" confidentiality or security, it would appear to trigger the proposed risk assessment requirements that are discussed further below.

Not-So-Safe Harbors

Once the definition of "security breach" is triggered (and, as described above, it's easy to do) an organization is not required to notify individuals of the breach if "there is no reasonable risk [of] harm." That harm threshold sets a much higher bar than most state corollaries and leaves open the possibility that the harm could be reputational (many state laws limit themselves to financial harms). Importantly, the proposal also would require organizations to document their risk assessment and submit it to the FTC. Failing to conduct a risk assessment "in a reasonable manner or according to standards generally accepted by experts in the field of information security" would constitute a statutory violation (brace yourselves for the onslaught of marketing around this potential new service offering . . .). Furthermore, the harm threshold imposes a de facto system logging requirement on any organization that wants to utilize the harm threshold. The logs must be submitted to the FTC with the risk assessment "as applicable and to the extent available." Those logs must cover the six months prior to the breach (which may exceed normal log retention periods maintained by many organizations), and they must reflect "each communication or attempted communication with a database or data system containing [SPII] . . . including any Internet addresses, and the date and time associated with the communication or attempted communication." The logs also must include "all log-in information associated with the databases or data systems containing [SPII], including both administrator and user log-in information." Let's hope that doesn't mean full network credentials . . .

The combination of the broad security breach definition, the high bar set by the harm threshold, and the burden of conducting and documenting a risk assessment with requisite log data may mean that most incidents of unauthorized access would result in notification to individuals.

The proposal also does not provide the popular "encryption safe harbor" available in virtually all other breach notification laws. The proposal provides that if SPII 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." Although that presumption would, at first blush, appear to broaden the opportunity to rely on technology-based safe harbors, its legal availability is much less certain. Specifically, the proposal provides that "[a]ny such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised." As such, the presumption that data were inaccessible is rebuttable and the analysis must be submitted to the FTC as part of the risk assessment. Organizations will not be at liberty to unilaterally determine the presumption is available.

Broad Types of Personal Information Covered

The proposal covers a much wider array of information compared to most breach notification laws. The definition of SPII covers several data elements when breached in combination with an individual's name, such as name plus date of birth plus home address; name plus a "security code" or "access code" (which is quite vague); or name plus mother's maiden name plus phone number. It also covers several types of data regardless of the inclusion of a name, such as a non-truncated Social Security number, driver's license number, passport number, or other government-issued unique identification number; unique biometric data such as a finger print, voice print, retina or iris image, or "any other unique physical representation" (again, quite vague); a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; and 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. The broad and vague drafting supports a conclusion that this proposal may promote the broadest coverage of personal information yet provided in a breach notification law. It also appears that the list of data covered was pulled together from multiple existing breach notification laws and past legislative proposals.

In case any bases were not covered by the currently proposed, fantastically broad definition, the proposal also provides that the FTC may modify the definition of SPII under certain conditions. That rulemaking authority could mean that the definition of SPII is revisited on a regular basis, which suggests breach notification obligations will evolve and likely expand if the measure survives and is enacted.

Incomplete Preemption

The proposal purports to supersede any "provision" of state law "relating" to the notification of breaches affecting "computerized data". In other words, the proposal may be intended to preempt state breach requirements concerning computerized data. Unfortunately, the preemption provision does not make clear how it affects state laws requiring notification of computerized and hard copy data. State notice requirements pertaining to hard copy data co-mingle their notice requirements with those applicable to computerized data. Thus, the hard copy requirement is "relat[ed]" to the computerized data requirement and arguably preempted if the proposal is enacted. However, the section of the proposal addressing preemption is susceptible to an argument that it was not intended to preempt state laws compelling notice of breaches affecting hard copy data because the proposal's preemption language, in addition to most other provisions of the proposal, appears wholly aimed at electronic data security.

The proposal also does not cover some types of information addressed by current state laws, such as health insurance or medical information. That lack of coverage may raise additional questions about preemption, but the gap may be of relatively short-lived import given that the proposal grants the FTC authority to designate additional information as SPII.

Notice to Individuals

When notice of the security breach is due to affected individuals, the proposal retains the dichotomy of most state breach laws, obligating third parties in

possession of SPII to notify the data's owner or licensor, which is then responsible for notifying affected individuals. Importantly, the proposal expressly provides that it will not prevent contractual agreements or other delegations to the contrary, meaning that a company can obligate its vendors to carry out notification in its stead. In such cases, the proposal would affirmatively excuse the data owner or licensor from its notification duties. However, the proposal also would require that notices name the business entity with which the individual has a "direct business relationship." As a result, even if a company obligates its vendor to carry out notifications, the company will need to be named in the notice if it, and not the vendor, holds that direct business relationship with the affected individuals.

Notice to DHS, FBI, and FTC

The requirement to submit a risk assessment to the FTC, as noted above, will automatically alert the agency to even non-notifiable potential security breaches. In addition, notice of the security breach may be required to an entity that will be designated by the Secretary of Homeland Security. That notice will be required if the breach affects more than 5,000 people; involves "a database, networked or integrated databases, or other data system containing [SPII] of more than 500,000 individuals nationwide"; "involves databases owned by the Federal Government;" or involves "primarily [SPII] of individuals known to the business entity to be employees and contractors of the Federal Government involved in national security or law enforcement." The entity receiving the notice on behalf of DHS is required to "promptly notify" the U.S. Secret Service, the FBI, and the FTC ("for civil law enforcement purposes").

Mandatory Notice to Media and No Substitute Notice

Under the proposal, if more than 5,000 persons residing in any state will receive notice of a security breach, then notice also would be required "to media reasonably calculated to reach such individuals, such as major media outlets" in the given state. Notably, the proposal does not provide a substitute notice method for situations such as when individual contact information is not available or the breach exceeds a certain size or cost.

Tricky Timing

The proposal provides that notice is due "without unreasonable delay." "Reasonable delay" may not exceed 30 days although the FTC is empowered to grant 30-day extensions "to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to [the DHS-designated] entity." The notifying organization can be required to present evidence of the need for delay. A 30-day delay also is available if a federal law enforcement agency determines that notification would "impede a criminal investigation or national security activity." That delay also may be extended by the federal law enforcement agency.

The notification to an entity designated by DHS (discussed above) must be provided as "promptly as possible" but at least 72 hours in advance of the notice to individuals, or 10 days after discovery of the incident, whichever is earlier.

Limited Exemptions

Let's begin by noting which organizations did not get an exemption: financial institutions subject to the Gramm-Leach-Bliley Act that comply with federal functional regulators' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Those organizations have benefited from helpful, in some cases partial, exemptions under current state breach notice laws.

But HIPAA-covered entities and vendors of personal health records can breathe a small sigh of relief. Both are provided a partial exemption because they are subject to federal breach notification requirement already in place due to the HITECH Act (the former under the U.S. Department of Health Human Services (HHS) breach rule and the latter under the FTC's breach rule). The exemption is partial, however, because the proposal would not grant those entities any relief with regard to their non-HITECH Act covered functions, which most notably means that breaches of employee SPII would be subject to this proposal (other than breaches by an employer health plan, which would presumably still be subject to HHS's breach rule).

Another important exemption is available in the interest of national security. The proposal provides that individual notice will not be required if the U.S. Secret Service or FBI determines that notification could reveal "sensitive sources and methods" or "similarly impede the ability of the agency to conduct law enforcement investigations." In addition, an exemption is available if the FBI "determines that notification of the security breach could be expected to cause damage to the national security." (The proposal would offer immunity from non-constitutional causes of action to these federal agencies, but not to the breached business entities, in the event the exemption is relied upon.) Obviously, these exemptions will not be available without consultation with the U.S. Secret Service or FBI.

A third, unusual exemption is provided for a business entity that (1) "effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual;" and (2) "provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions." This exemption appears to be aimed entirely at breaches affecting payment cards, and that assumption seems to be confirmed by an express limitation in the proposal that excludes from the exemption any breach affecting "the individual's first and last name or any other type of sensitive personally identifiable information other than a credit card number or credit card security code." Whether intentional or not, based on that language, the exemption is apparently unavailable for debit cards and also unavailable if the breach affects full track data from a credit card.

Importantly, the two exemptions discussed immediately above (the "national security exemption" and the "credit card" exemption) will only exempt entities from notifying affected individuals. Notice to federal agencies (discussed above) would apparently be required notwithstanding the availability of these two exemptions.

Enforcement

The proposal provides that violations would constitute unfair or deceptive trade practices, enforced by the FTC. Since the FTC also would have broad rule-making authority to issue virtually any regulations it deems necessary to effectuate the law, violations of those future rules would be subject to monetary penalties. State attorneys general also have enforcement authority, including the option to impose civil penalties of up to $1,000 per day, per individual whose sensitive personally identifiable information was affected, up to a maximum of $1,000,000 unless the conduct in question was willful or intentional. The proposal does not include a private right of action.

What's Next?

Tune in for the President's State of the Union address to find out more about his proposals on privacy and cyber security. Whether or not the proposed Act is carried forward may depend on whether members of Congress decide to reintroduce past proposals on the same topic.