McDonald Hopkins
A business advisory and advocacy law firm®
ALERT
DATA PRIVACY AND CYBERSECURITY

January 28, 2015

I'm just a bill. Yes, I'm only a bill.

But what if the Personal Data Notification & Protection Act passes?

On the immediate heels of the Sony hack (not to mention a few other sizeable breaches), the White House introduced the Personal Data Notification & Protection Act (PDNPA) as part of its agenda to further privatize data and improve cyber security. This is certainly not the first federal cyber security law to be proposed, but it is the only one to have the White House's clear stamp of approval.

Comparing the PDNPA to some of the other proposed laws, there are clearly some similarities, but what is most striking about the proposed PDNPA are the key differences. For instance, if passed, the PDNPA would apply to a much broader set of information that the PDNPA defines as "sensitive personally identifiable information" (SPII). This, however, is not the only key difference.

In an effort to provide some much-needed clarification on the proposed law, we put together the following list of FAQs that address what would happen if the PDNPA passes.

What would be considered a security breach?

The PDNPA defines a "security breach" as a "compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in the unauthorized acquisition of [SPII] or access to SPII for an unauthorized purpose, or in excess of authorization" or if there is a reasonable basis to conclude either.

One foreseeable issue with this language is that it does not include an exception for employees or agents who mistakenly, but in good faith, access SPII without sufficient authorization. This is an extremely common type of unauthorized access that many of the corollary state statutes specifically address. The PDNPA, however, does not include this exception, which means the occurrence of this type of unauthorized access would trigger the risk assessment and potentially the notification requirements.

What information would be covered under the PDNPA?

The PDNPA would consider any unauthorized acquisition of or access to SPII as a security breach. The definition of what actually constitutes SPII is quite broad (broader than any definition previously proposed), and would include any compilation of information, in electronic or digital form, that meets any one of these six definitions:

1. An individual's first and last name or first initial and last name in combination with any two of the following: (a) home address or telephone number; (b) Mother's maiden name; or (c) full birth date.
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 finger print, voice print, retina or iris image, or any other unique physical representation.
4. A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code (notably this does not include the requirement that an access or security code be coupled with the number).
5. A user name or email address, in combination with a password or security question/answer that would permit access to an online account.
6. A combination of the following three 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.

If these categories were not broad enough, the PDNPA would also allow the Federal Trade Commission (FTC) to modify the definition under certain conditions, which means the definition of SPII would be subject to change and evolve.

One issue with the PDNPA's definition of "security breach" is that, unlike many of the state laws, it does not include an exception for employees or agents who access SPII by mistake, without authorization, but in good faith. While this type of

unauthorized access would likely not compromise confidentiality or security – another requirement in the definition of security breach – it would appear to set off the risk-assessment requirement, which is discussed below.

What would a business have to do if it suffers a security breach?

A business that suffers a security breach would be required to send a number of notices, as follows:

Individual Notice

If a security breach occurs, a business entity would be required to give notice to the individual whose SPII has been, or is reasonably believed to have been accessed or acquired within 30 days of discovering the security breach. The only exception to this is if "there is no reasonable risk of harm or fraud" to that individual. Mail, telephone, or email notice (if the individual has consented and the notice complies with the ESIGN Act) are sufficient.

The proposed law would obligate third parties in possession of SPII to notify the data's owner or licensor, who is then responsible for notifying affected individuals. The PDNPA would not prevent contrary contracts or other assignments. What this specifically means for businesses is that they could contractually task their vendors with the notification responsibility and effectively excuse the data owner or licensor from its notification obligations. Any notices, however, would have to contain the name of the business entity with which the individual has the "direct business relationship." Practically speaking, this means that even if a company contractually requires its vendor to provide necessary notifications, the company will still be named in the notice if it holds the direct business relationship with the affected individuals.

The notice threshold appears higher than most state laws require and would be triggered in cases of reputational harm. In contrast, many state laws are only triggered when there is risk of, or actual, financial harm.

One noteworthy point about the notification requirement is that the PDNPA would only apply to businesses that use, access, transmit, store, dispose of, or collect SPII about more than 10,000 individuals during a 12-month period. This would exempt many small businesses from the individual-notice requirement.

Businesses that are required to provide health-related breach notifications under the Health Information Technology for Economic and Clinic Health Act (HITECH) would also be exempt from these notification requirements.

A business would be exempt from the individual notice requirement if it conducts a risk assessment and concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose SPII was subject to the security breach. In addition, to take advantage of this exception, the business entity must notify the FTC in writing of (1) the results of the risk assessment, and (2) its decision to invoke the risk assessment exemption not later than 30 days after the discovery of a security breach. One may question what the FTC will do with the risk assessments it receives. Will the FTC review them? What if the FTC comes to a different conclusion; i.e. there was a risk of harm and notice should have been given.

Government Notice

Businesses would have to notify federal law enforcement and national security authorities of a security breach if:

(1) The SPII of more than 5,000 individuals was accessed or acquired;
(2) The breach involved a data system containing sensitive personally identifiable information of more than 500,000 individuals nationwide;
(3) The breach involves databases owned by the federal government;
(4) The breach primarily involves SPII of federal employees and contractors who are involved in national security and law enforcement.

Media Notice

Media notice would be required if a security breach resulted in the disclosure of SPII of more than 5,000 individuals in one state. The notice itself must be "reasonably calculated to reach such individuals," which would include notice to major media outlets in the affected states. If passed, this requirement would be a significant change from the existing state laws, which only require media notice as an alternative way to notify.

Credit Reporting Agency Notice

If a breach involves more than 5,000 individuals, businesses would have to notify all consumer reporting agencies of the timing and distribution of the notice within 30 days, unless an extension is received.

What is the timeframe for any required notice?

The proposed law would require that any notice be given without "unreasonable delay," which may not exceed 30 days. The

FTC, however, would be authorized to grant 30-day extensions "to determine the scope of a security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to [the Department of Homeland Security-designated] entity."

What about all of those state laws on this issue? What happens to them?

Currently there are 47 states that have breach notification laws. For businesses trying to comply with them, doing so has become quite tenuous because not only do they differ, but some even impose contradictory requirements. The PDNPA purports to preempt any provision of any state law that relates to the notification of breaches affecting electronic information. However, states would still be allowed to require notices to include information regarding state-provided victim protection assistance.

One point worth noting is that, because the proposed PDNPA only applies to "computerized data," there appears to be a gap between the PDNPA and many of the state laws because the PDNPA does not appear to include hard copy data that many of the state laws address. As it is currently written, if the PDNPA were to pass, businesses would have to follow the PDNPA in regards to notification requirements for security breaches of electronic data, but continue to follow any applicable state law if there is any breach of hard copy data.

Who would be covered?

There are very few exceptions or exemptions, which are discussed below. What this means is that many businesses, including financial institutions subject to the Gramm-Leach-Bliley Act that have to comply with federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and other business that benefited from partial exemptions under many current laws, would be subject to this law.

Who would not be covered?

Although it can be gleaned from the notification information above, it is worth noting again that small businesses that do not use, access, transmit, store, dispose of, or collect SPII of more than 10,000 individuals in a 12-month period would be exempt from the notification requirements of the proposed law.

HIPAA-covered entities and vendors of personal health records and business entities covered by the HITECH Act are partially excluded. The proposal would not give these businesses any exclusion from their non-HITECH duties, which means that breaches of employee SPII (as opposed to breaches by an employer health plan) would be subject to the PDNPA.

The PDNPA would also exempt any business entity that (1) effectively blocks the use of the SPII to initiate unauthorized financial transactions before they are charged to the account of the individual, and (2) that provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions. This exemption seems to be aimed specifically at breaches affecting payment cards, not debit cards or breaches affecting full track credit card data.

Who enforces it?

The FTC, in consultation with the U.S. Attorney General, would be able to initiate an investigation into a business's compliance with the law. The proposed law provides that violations would constitute unfair or deceptive trade practices. State attorneys general would also be able to bring civil actions on behalf of their residents and seek injunctive relief or civil penalties of up to $1,000 per day per individual with a maximum $1 million per violation unless the conduct has been found willful or intentional. The proposed law does not include a private right of action.

Takeaway

Rather than simplify the breach notification landscape, the PDNPA, in its current state, would appear to create more uncertainty and generate more questions than answers. However, it is certainly receiving the most hype of any federal breach notice bill proposed in the past. But what will be the outcome? The effect on the 47 different state breach notice laws will be the most critical component of the Act. As currently written, and inclusive of all of the gaps, passage of the PDNPA may just increase the number of breach notice laws by one and complicate the legal landscape even further. McDonald Hopkins' national data privacy and cybersecurity team, along with McDonald Hopkins Government Strategies, will continue to track the PDNPA as it makes its way through Congress and provide continuing updates.

For more information, please contact:

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Sara Hutchins Jodka
614.484.0716
sjodka@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

Data Privacy and Cybersecurity

Our national Data Privacy and Cybersecurity team has a wealth of experience advising clients on best practices for data privacy, security, storage, and disposal. We specialize in breach coaching clients through the myriad of rapidly changing state, federal, international, and industry privacy and breach notification laws, including drafting and implementing proactive measures and employee training. Our skilled attorneys also provide client support during investigations by state and federal regulators. We have significant expertise in litigation prosecution (indemnification) and litigation defense (single plaintiff and class action). Our attorneys deal with data breaches every day. The national Data Privacy and Cybersecurity team at McDonald Hopkins has counseled clients in nearly every industry through hundreds of privacy incidents. When a data breach occurs, it's fast moving and there's no time to spare. We are here to advise your organization and advocate for your business. We don't just practice data privacy law. We live data privacy law 24/7. If you suspect that your organization has suffered a data breach or privacy incident, call our 24/7 Hotline at 855-MH-DATA1 (855-643-2821).

McDonald Hopkins LLC

A business advisory and advocacy law firm®

Carl J. Grassi, President
600 Superior Avenue, East, Suite 2100, Cleveland, Ohio 44114

Chicago 312.280.0111 Fax: 312.280.8232	**Cleveland** 216.348.5400 Fax: 216.348.5474	**Columbus - North Fifth Street** 614.484.0700 Fax: 888.671.1828	**Columbus - South High Street** 614.458.0025 Fax: 614.458.0028
	Detroit 248.646.5070 Fax: 248.646.5075	**Miami** 305.704.3990 Fax: 305.704.3999	**West Palm Beach** 561.472.2121 Fax: 561.472.2122