President Obama's New Personal Data Notification & Protection Act: Overview, Analysis, and Challenges

Webinar Q & A - February 12, 2015

On January 12, 2015, President Obama proposed a new piece of legislation, the Personal Data Notification and Protection Act (PDNPA), which would establish national standards for data breach notification. But there is much that is unclear about the Act, its chances for passage, and how it might impact more rigorous state regulations. This webinar, held on February 12, 2015, explored the provisions of the Act, looked at it in context of the existing environment of other state and federal laws and a newly seated Congress, and provided advice to organizations related to their own privacy and data protection priorities in the interim.

Here are the questions that were posed by the attendees and answered by presenters Dominic Paluzzi and James Giszczak of McDonald Hopkins.

Do you know whether the definition of "business entity" under the proposed legislation--and particularly the "organization" term--includes states? Does it include federal agencies?

The current definition of "business entity" in the PDNPA does not appear to include states or federal agencies. The terms appear to only encompass entities that may be organized via a state's business laws, not an entity that is the state or federal government.

When you say "at the time of the breach," do you mean the time period the breach occurred, or the date the breach was detected?

The date the breach was detected. Some breaches begin months before they are ever detected. A business entity's notification obligations would only start running from the date the entity discovers the breach. In particular Section 101(a) of the PDNPA provides in relevant part: "[a]ny business entity…shall, following the discovery of a security breach, notify any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual."

Is health data excepted too?

Businesses acting as covered entities, business associates, or third-party service providers subject to HIPAA/HITECH are exempted from coverage. There is no exemption, however, for breaches of employee sensitive personally identifiable information (SPII) at a covered entity or business associate.

How does the preemption clause impact state statutes that have intermingled notification requirements for data and hardcopy breaches?

The PDNPA is silent relative to hardcopy/paper data breaches and only covers "computerized data." To determine whether PDNPA would apply, or whether the state laws apply, depends on whether the breach involved computerized data or hardcopy data.

If an SSN with no name is needed to be called PII… what's the difference between an SSN and any 9-digit number? If I had a list of 9-digit numbers stolen I could just argue they were not SSNs, maybe they were random 9-digit numbers of French phone numbers.

One is a Social Security number that the business entity has specifically gathered for purposes of doing business. They would arguably also be kept in a database or in a form that would identify them as Social Security numbers other than just random 9-digit codes. When tracing where the breach started and where the information was obtained, the computer forensic analysis should be able to determine what database was impacted. If it is only containing Social Security numbers, then there has been a security breach. If it is a database containing French phone numbers, it would only be a breach in the event it is also connected with an individual's first and last name or first initial and last name. See Section 1(h)(1)(A).

Shouldn't companies with a presence in multiple states be using the strictest standard across the board instead of looking to each states' standards (until any federal regulation preempts those standards) as a best practice?

This approach makes sense relative to proactive, preventative compliance. As to breach notification requirements, however, you cannot use the strictest standard and apply that for all states as the requirements for content, timing and notice all differ. You will be in violation of certain state statutes if you apply the "strictest" standard to all.

If it does not mention state entities or federal entities, is it possible they are still included under the "organization" term?

The PDNPA appears to only apply to businesses, for and non-profit. There is no indication that it is meant to apply to state or federal governments.

Does the 10k individual standard apply only to the interstate commerce itself? Or would it apply to ANY large enterprise with 10,000 or more employees that is engaged in interstate commerce and, by its normal operations, collects SPII on its employees?

The 10K individual standard does not apply to the interstate commerce itself as there is an additional component – the disposal or collection requirement. The 10,000 number is the number that would trigger notification, but that number is determined as follows: the business entity must be disposing of, or collecting, sensitive personally identifiable information about more than 10,000 individuals during any 12-month period. The 10,000 number is not about a number of employees per se; however, if the business entity is disposing of or collecting SPII on more than 10,000 employees during any 12-month period, then it would be covered.

Are there exceptions to the notification timeline if there is an ongoing investigation, and notification may hamper the investigation?

Yes. If the FBI or Secret Service determines that notice would reveal sensitive sources or methods or damage national security there may be a complete exemption from having to provide notice altogether. If an organization receives a written stay of notice pending a law enforcement investigation, the organization must notify affected individuals within 30 days once the delay is invoked, unless the feds indicate a further delay is necessary.

The proposal doesn't really acknowledge the role of vendors--that is, what happens when my vendor (or worse, a subcontractor of a vendor) tells my company about a breach on day 29? What is the group's experience with vendors and thoughts on this statute?

You are correct; the PDNPA does not require vendors to notify owners within a certain period. Florida did a great job addressing this in its recent amendment to the Florida Information Protection Act (requiring vendors provide notice to owners of data breach within 10 days, allowing the owner at least 20 days to meet the 30 day notice requirement in Florida). Nearly a third of all breaches are the result of the vendor having the breach, so this is a critical provision that is missing in the PDNPA.

If a 3rd party is breached, who bears the cost of notification? 3rd party or the entity that has the relationship with the consumer?

The business entity that disposes of or collects the information is responsible for notification to any an individual whose SPII has been access or acquired; however, a business entity may enter into an agreement with a designated third party, including an owner or licensee of the SPII to provide the notifications instead. Section 101(b)(2). In addition, a business entity that is required to give notice is fully relieved from giving notice if an owner or licensee of the SPII or other designated third party provides the notification, and names the business entity (owner of the data) in the notice. Section 101(b)(3).

What about if you have a BAA that requires the Business Associate to provide the notice to the affected individuals? Will this provision overwrite that? We have BAAs that require the BA to send notice, which must be approved by us before the BA sends it.

That is acceptable under the PDNPA, except that your BAA must mention your organization's name in the notice letter, assuming your organization has the direct relationship with the affected individual receiving the notice letter.

Does the bill give a description of how to conduct a risk assessment or what must be considered when doing a risk assessment? For example, HIPAA delineates 4 factors for doing a risk assessment.

Unfortunately, no. The PDNPA should model some type of test (although some may argue the Final Rule 4 factor test is not the best model).

Does encryption of SPII provide any provision of "safe harbor"?

Not automatically like it does under some state notification laws. Under the PDNPA, in the event of a security breach, a business entity is only exempt from the notification requirement if it conducts a risk assessment and concludes there is no risk that the security breach has resulted in, or will result in, harm to the individuals whose SPII was subject to the breach. If the data at issue was rendered unusable, unreadable, or indecipherable, like through encryption, there is a presumption that no risk exists, but the risk assessment will still have to be performed and the business entity will still have to inform the Commission of the results of its risk assessment and its decision to invoke the risk assessment exemption. This must occur not later than 30 days after the discovery of a security breach, unless extended by the Commission. Section 102(b)(1).

I'm still confused. I represent a small nonprofit foster care, mental health counseling, and adoption agency. Total caseload is less than 700 and total staff is less than 100. Are we still required to comply with this coming PDNPA law?

Only if the business entity disposes or collects SPII on more than 10,000 individuals in any 12-month period. While they are still a small non-profit, they still likely engage in interstate commerce, as the term is defined quite broadly, meaning the only way to avoid adherence to the law would be by not hitting the more than 10,000 number.

On the discussion of "computerized data," is that term not broad enough to cover data in printed form that has been manipulated by a computer, e.g., a printout of an Excel spreadsheet?

The PDNPA does not define "computerized data," but state regulators have certainly made the argument that that term encompasses hardcopy data that was printed from a computer and exists somewhere in a computerized format.

Is there a statutory bar on lawsuits, or language that says the statute does not create a COA?

The PDNPA does not include a private right of action for individuals affected by a security breach like some state notification laws allow. Rather, the only type of actions that can be brought for violations of the PDNPA are those pursued by the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or State statute to prosecute violations of consumer protection laws. The remedies allowed include injunctive relief and civil penalties of not more than $1,000 per day per individual whose SPII was, or reasonably believed to have been, accessed or acquired by an unauthorized persons, up to a maximum of $1,000,000 per violation unless the conduct is found to be willful or intentional. Before an attorney general or other allowed actor can file such a suit, they must provide written notice and a copy of the Complaint to the Attorney General and the Commission.

Would the owner of the data need to notify about the breach if the data was masked?

Having the data "masked" is not an automatic bar to require notification as is would be under certain state notification laws. Under the PDNPA, in the event of a security breach, a business entity is only exempt from the notification requirement if it conducts a risk assessment and concludes there is no risk that the security breach has resulted in, or will result in, harm to the individuals whose SPII was subject to the breach. If the data at issue was rendered unusable, unreadable, or indecipherable, like through encryptions, there is a presumption that no risk exists, but the risk assessment will still have to be performed and the business entity will still have to inform the Commission of the results of its risk assessment and its decision to invoke the risk assessment exemption. This must occur not later than 30 days after the discovery of a security breach, unless extended by the Commission. Section 102(b)(1).

Is the FTC equipped to enforce this legislation? And is the legislation going to be able to be flexible as technology changes and data companies collect and share changes?

As currently staffed, likely not. However, in their 2016 budget request, they asked for a $309,206,000 program level with 1,191 full-time equivalent positions. It is unclear how flexible the legislation will be as technology changes. This particular law, however, is not a technology intensive law and does not so much depend on what is going on with technology. With that, it seems intended to withstand technology changes. If you read the bill, there is very little technological terms.

Is there a possibility that the preemption clause would mean that businesses that collect information on less than 10,000 people would not be subject to state laws that would have previously applied? Or would they definitely still be subject to state laws?

Nothing is for certain relative to this pending bill. But, we doubt the intention was to relieve small and mid-sized organizations from having to comply with any breach notice requirements.

Do the bill's requirements apply to government agencies? If not, has there been discussion of how applicability would play out in the case of a private entity performing under contract with a government agency?

States agencies and public entities are, arguably, not covered by the PDNPA. There have been no public discussions regarding this component, as of yet.

What is the likelihood of this legislation passing and would it supersede state laws such as HB300 here in the State of Texas?

It would preempt the states' current breach notification laws as they cover and apply to a business engaged in interstate commerce of a security breach. The remainder of the state law, and any notification for non-covered entities under PDNPA would still be covered under any applicable state law.

Does the POTUS's plan move the US towards more or less conformity with EU regulation?

Less conformity with EU regulation. The EU has different focuses than the President's current initiatives, which concern mainly consistent breach notification standards, protection of student data, consumer privacy, and collaboration and information sharing between private entities and the government. The EU's focus is vastly different and focuses on implemented security measure to prevent breaches, increasing critical information infrastructure protection, protection of children, etc.

What's the status of this law?

The law was just proposed in January 2015. It has yet to make it before Congress or for committee debate.

We are a covered entity and subject to HITECH. Would we really be exempt from this proposed bill?

Businesses acting as covered entities, business associates, or third-party service providers subject to HIPAA/HITECH are exempted from coverage. There is no exemption, however, for breaches of employee SPII at a covered entity or business associate. Certainly, as a covered entity, you would still be required to provide notice of a breach to affected individuals, the media, and HHS OCR, under the Final Rule.

Can you tell me whether under the PDNPA a breach is presumed and reportable when a laptop or other device is lost or stolen and a risk assessment including but not limited to cyber forensic analysis cannot be performed to validate if SPII was breached?

You bring up an interesting point and this relates to a previous question about the guidelines for the risk assessment (or the lack thereof). Although the bill, as proposed, does not provide for requirements of the risk assessment, you can still perform a risk analysis using your hypothetical. Although you cannot perform a forensic analysis since you do not have the computer in your possession, it could be argued that since the laptop was stolen and no longer in your possession, there is a risk of harm to the SPII and notice would be required.

Talk to an Expert

971-242-4775 | Info@IDExpertsCorp.com

McDonald Hopkins
A business advisory and advocacy law firm

About McDonald Hopkins

McDonald Hopkins 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.

id experts®

About ID Experts

At ID Experts®, we provide innovative software and services that simplify the complexities of managing data incident response and reduce breach risks. Our breach response services—including YourResponse, our unique breach response process—are tailored to the needs of our breach clients, their counsel, and insurer. Since 2007, our team of certified experts has managed breaches for some of the nation's largest healthcare, financial services, retail, higher education, and government organizations.