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

January 14, 2015

President Obama's new data privacy agenda

Focuses on two laws that aim to put the privacy back in "data privacy"

President Obama recently spoke to the Federal Trade Commission about his privacy and data security agenda. The agenda included a series of voluntary partnerships, but the cornerstone was two privacy acts that will soon be sent to Congress: The Personal Data Notification and Protection Act and the Student Digital Privacy Act.

The Personal Data Notification and Protection Act

Little is currently known about what the Personal Data Notification and Protection Act will ultimately require and mean for businesses, but it appears that the key focus would be to create a national data breach notification standard that would require businesses to notify their customers within 30 days of discovering a breach of personal information.

Many businesses – especially those who collect data from customers across many states – may welcome a nationwide breach notification standard. Given that the state of residency of the affected individuals currently dictates which law applies, organizations often struggle to comply with the patchwork of 47 individual state breach notification laws, which vary significantly. Only three states do not currently have data breach notification laws: Alabama, New Mexico, and South Dakota.

Many businesses, however, are not happy with the proposed 30-day notification timeframe because it is a short period of time to comply and coincides with some of the strictest state-law notification requirements.

A key point about the proposed law that remains unclear is whether it will expressly preempt state data breach notification laws (similar to how ERISA works in the state-law context). Or, whether it will merely set a minimum standard and leave the states to enact or continue on with their own stricter laws (like states are allowed to do in establishing higher minimum wage rates).

Many commentators believe the law will preempt the multitude of state laws. It is foreseeable that most businesses will welcome this universal standard, but some may worry that it will allow for a weaker standard than what some of the state laws currently have and preclude the states from enacting or retaining stricter, stronger protections. Also, the various state attorneys general may lose enforcement power and the ability to levy fines and penalties.

One thing that is clear is that the proposed law would give the Federal Trade Commission the authority to enforce it and allow the agency to levy penalties upon businesses who fail to comply. If passed, the law would also criminalize the international trade of illegally-obtained personal information.

The Student Digital Privacy Act

The Student Digital Privacy Act seeks to protect student data as educational institutions embrace newer technologies. The draft bill would prohibit private companies from profiting from the sale or use of student data collected in the educational context. The use of information for targeted ads was specifically addressed.

These proposed laws and the timing of President Obama's announcement are no surprise given the state of cyber affairs in this country. Not only do they follow the President's levying sanctions against North Korea related to the Sony hack, but going back much further, they coincide with the White House's call for a federal Consumer Privacy Bill of Rights, which was proposed in a February 2012 whitepaper titled "**Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital Economy**." Now, the period for public comment on it is complete, and the Commerce Department has announced it will release the proposal within 45 days and has asked that Congress begin consideration of it. It is likely that the White House will send the two proposed laws to Congress around the same time Congress looks to consider the Commerce Department's proposal.

Takeaways

Data privacy and cybersecurity are critical issues for both individuals and industry, and rightfully so. If Sony and the myriad of other breaches have taught us anything, it is that no business with a computer network (or Internet access) is safe from a cyber attack. Even without an attack, no business is flawless, and there are simply too many ways private information can become … well, not so private. In addition, no electronic information is off limits. Whether it be personally identifiable

information, protected health information, financial information, trade secrets, internal company documents, or even high- or low-level employee emails, etc., information has value, and there is a market for anything with any value. As businesses continue to wrap their heads around these issues, they should expect to soon put federal-legislation compliance on their to-do lists.

For more information, please contact:

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

Sara H. Jodka
614.484.0716
sjodka@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