McDermott Will & Emery

The White House Calls for Action Where Congress Has Failed to Deliver

An In-Depth Analysis of President Obama's January 2015 Proposals on Privacy and Security

February 12, 2015

SPECIAL REPORT

McDermott Will & Emery

SPECIAL REPORT

For more information, please contact your regular McDermott lawyer, or:

Heather Egan Sussman
+1 617 535 4177
hsussman@mwe.com

Amy C. Pimentel
+1 617 535 3948
apimentel@mwe.com

Jennifer S. Geetter
+1 202 756 8205
jgeetter@mwe.com

David Ransom
+1 202 756 8089
dransom@mwe.com

Ann Killilea
+1 617 535 3933
akillilea@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com

Table of Contents

On January 12 and 13, 2015, U.S. President Barack Obama made two announcements regarding the White House's continued work to address evolving issues in privacy and security. The first announcement, titled Safeguarding American Consumers and Families, outlines steps the administration is taking to address important issues of personal privacy, including proposing legislation to protect student privacy. The second announcement, titled Securing Cyberspace, reintroduces and reframes three legislative proposals made to Congress, and announces other steps aimed at protecting the government, the economy and the United States.

While some aspects of the administration's proposals, such as student privacy, are noncontroversial and will likely gain traction in this Congress, others, such as efforts to enact an omnibus federal privacy law grounded in a "Consumer Privacy Bill of Rights," appear to have little hope of succeeding. While some critics complain that the president has released nothing new, others applaud the president for continuing to advance the ball on important modern issues, such as cyber threat information sharing, on which Congress has been reluctant to act. These supporters suggest to Congress that it "should use this plan as a guideline, and improve upon it to craft significant legislation that further cultivates the public-private cyber threat partnership."

This *Special Report* provides an overview and analysis of the two plans and explains their impact on U.S. companies.

The President's Plan for Securing Cyberspace

On January 13, 2015, the day after releasing the president's proposed action plan on consumer privacy (discussed below), the White House released a proposed plan for Securing Cyberspace. The plan is likely to be debated at a White House Summit on February 13, 2015, hosted by Stanford University, which will bring together public and private sector stakeholders to help shape a national response to these threats. The guest list is tightly controlled by the White House, but Stanford reports in its press release that "the all-day event will include senior leaders from the White House and across federal government; CEOs from a wide range of industries including financial services, technology, retail and communications companies; law enforcement officials; and consumer advocates."

The president's Securing Cyberspace plan authorizes the U.S. Department of Energy to award $25 million in grants over the next five years to 13 universities designated as Historically Black Colleges and Universities (HBCUs). These grants are intended to support a cybersecurity education consortium.

The plan also consists of three legislative proposals, which were delivered to Congress on January 13, 2015:

- The Personal Data Notification and Protection Act
- Proposed legislation on cybersecurity information sharing
- A proposal to amend certain law enforcement provisions of existing laws, which will
  - Make it easier to prosecute organized crime groups that utilize cyber attacks
  - Deter development and sale of computer and cell phone spying devices
  - Modernize the Computer Fraud and Abuse Act
  - Ensure that courts are authorized to shut down botnets

Each of these three legislative proposals, discussed in greater detail below, is designed to improve the United States' ability to combat cyber threats.

The Personal Data Notification and Protection Act

The administration proposed new legislation titled the Personal Data Notification and Protection Act (Breach Notification Act), which sets forth a national data breach notification standard. This proposal defines what a security breach is, outlines circumstances under which a company must notify affected individuals and the government, and lists certain requirements with which companies must comply in the aftermath of a breach. The proposal provides that violations will constitute an unfair or deceptive act or practice under the Federal Trade Commission (FTC) Act and be subject to enforcement by the FTC and state

attorneys general. A state attorney general may bring an action if there is reason to believe that an interest of the residents of its state has been threatened or adversely affected by a violation of the Breach Notification Act.

DEFINITIONS

The Breach Notification Act establishes the following key definitions:

- A "business entity" is any organization, regardless of whether it is established to make a profit. Business entities that are subject to the Health Information Technology for Economic and Clinical Health Act are exempt from the Breach Notification Act, including its notification requirements.
- A "security breach" is a compromise of the security, confidentiality or integrity of computerized sensitive personally identifiable information. Notably, authorized investigations and intelligence activities conducted by federal, state or local governments are not considered security breaches.
- "Sensitive personally identifiable information" (SPII) includes the following:
  - First and last name in combination with any two of the following:
    - Home address or telephone number
    - Mother's maiden name
    - Date of birth
  - Non-truncated government-issued ID number (*i.e.*, driver's license number)
  - Unique biometric data (*i.e.*, fingerprints)
  - Unique account identifier (*i.e.*, bank account number)
  - User name or e-mail address in combination with a password or security question and answer that would permit access to an online account

This definition of SPII is particularly notable because it signals an evolution in U.S. terminology. It appears to be the first time an effort has been made to codify a category of SPII. Most U.S. state laws traditionally have called this type of data that can lead to identity theft or fraud some variation of "personal information" (PI) or "personally identifiable information" (PII), and each state has built its own special protections for this type of information. In contrast, European-style privacy laws are designed to protect "personal data," which generally is defined as any information that identifies or can be used to identify a living person, but also apply heightened protections to certain categories of "sensitive personal data."

The administration's proposed Breach Notification Act would effectively change the United States' vernacular approach—instead of categorizing data that deserve special protection as PI or PII, the Breach Notification Act would define this type of data as "sensitive personally identifiable information" similar to the EU terminology, but still with different definitions. This is a step in the right direction for an administration that continues to seek common ground between U.S. and EU privacy laws.

NOTIFICATION REQUIREMENTS

Following discovery of a security breach, the Breach Notification Act requires notification only if the breached entity uses, accesses, transmits, stores, disposes of or collects SPII about more than 10,000 individuals during any 12-month period. Thus companies that process the SPII of fewer than 10,000 individuals during any 12-month period would not be covered by this law, which deviates substantially from most state laws that do not have a minimum threshold for coverage.

Notification must meet the following requirements:

- Be made *without unreasonable delay*, meaning within 30 days of discovery of the breach, unless the entity seeks additional time from the FTC
- Be in the form of mail, telephone or e-mail (if prior consent was given)
- Contain a description of the SPII at risk; a toll-free number where consumers may ask questions; toll free numbers for the consumer reporting agencies, the FTC and the relevant state authority (if state law

requires as much); and the name of the business entity that has the direct business relationship with the individual

Media notice is required when the number of individuals involved in any one state exceeds 5,000. Notification to consumer reporting agencies is required if more than 5,000 individuals total are involved.

Notification must also be made to an entity designated by the secretary of homeland security, who must promptly notify the Secret Service when the breach involves the following:

- More than 5,000 affected consumers
- A database with more than 500,000 individuals
- A federal agency
- Information known by the breached entity to include SPII about federal government or federal contractor employees working in national security or law enforcement

RISK ASSESSMENTS

The breached entity would *not* need to make the required notifications if it conducts a risk assessment in a "reasonable manner" pursuant to generally accepted standards and concludes that "there is no reasonable risk that [the] security breach has resulted in, or will result in, harm to the individuals whose [SPII] was subject to the security breach." A presumption of "no risk of harm" is applied when the data was encrypted or otherwise rendered unusable through a security technology that is generally accepted by security experts at the time of the breach. This presumption is rebuttable with facts showing that the technology was circumvented.

Conducting a risk assessment acts as a safe harbor from the notification requirements. In order to invoke this safe harbor, a business that conducts a risk assessment and finds that there is no reasonable risk of harm must notify the FTC within 30 days of the results of the risk assessment. The risk assessment safe harbor is arguably the most important exemption for businesses in the Breach Notification Act, because it allows for a self-directed, proactive approach to breach response.

The Breach Notification Act includes two additional built-in exemptions to its notification requirements:

- When the U.S. Secret Service or Federal Bureau of Investigation determines that notification might reveal sensitive sources of information or impede the ability of the agency to conduct investigations
- When an entity utilizes a security program that effectively blocks the use of SPII before the initiation of an unauthorized financial transaction and provides notice of this unauthorized attempt

PREEMPTION

The Breach Notification Act provides that it supersedes any provisions of state law "relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data." Because the Act would only preempt laws related to *computerized* data, existing state laws requiring notification of breaches involving paper records would remain intact.

Similarly, state laws imposing minimum data security requirements likely would remain intact under this proposed legislation. At least 12 states currently have laws that require businesses to take affirmative steps to protect the personal information with which they come in contact. Because the administration's proposed legislation does not include minimum data security requirements, these state law provisions likely would not be preempted.

LOOKING AHEAD

On January 27, 2015, the House Subcommittee on Commerce, Manufacturing and Trade held a hearing to define the elements of a proposed data breach notification law. Despite the general push for federal preemption and a streamlined breach standard, disagreement remains regarding some of the details. The matters under discussion include the effect of having a harm-based notification trigger, the prospect of over-notifying individuals, what event or knowledge will trigger the start of the 30-day

breach notification period, and how long after the bill becomes law it should take effect.

If the Breach Notification Act does become law, companies will face a national standard for security breaches involving computerized SPII. This will simplify the competing categories of "personal information" separately prescribed by state law. Multinational organizations will be able to tailor their data breach response plans to one category of data, "sensitive personally identifiable information." Given the short deadline for notice, however, it will be important for companies to have systems in place that can quickly identify a breach, perform a risk assessment, and, if necessary, create and send required notices. Companies will also need to analyze relevant state laws to assess whether any more stringent state requirements will apply.

Proposed Legislation on Cybersecurity Information Sharing

The president's second legislative proposal updates a 2014 bill on cybersecurity information sharing. This effort had failed to gain traction in Congress previously. It seeks to codify mechanisms that will facilitate the sharing of cyber threat information between government and private entities, as well as among private entities. Many entities wish to share information with the government but are concerned about potential liability and the possibility of the information they share being further disclosed beyond their control. This legislation would clarify that private entities can indeed share information with each other and with the U.S. Department of Homeland Security (DHS) without fear of civil or criminal liability. It would put in place a framework for ensuring the privacy and security of any information that is disclosed. The legislation also encourages formation of private-sector-led information sharing and analysis organizations.

The goal of the legislation is to remove actual and perceived barriers to information sharing in order to incentivize public and private sector entities to share threat information in "real time" to better respond to cybersecurity incidents. Of all the president's legislative proposals released as part of the 2015 announcements, the updated cybersecurity information sharing legislation likely will receive the most attention initially by Congress, but the liability provisions could complicate the debate and slow its momentum.

DEFINITIONS AND CREATION OF A PORTAL

The legislative proposal contains a number of definitions, but the most important of these is "cyber threat indicator," because that is the type of information this legislation targets. In particular, "cyber threat information" is any information

- That is necessary to indicate, describe or identify
  - Malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat
  - A method of defeating a technical or operational control
  - A technical vulnerability
  - A method of causing a user with legitimate access to an information system or information that is stored on, processed by or transiting an information system inadvertently to enable the defeat of a technical control or an operational control
  - Malicious cyber command and control
  - Any combination of the above
- From which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat

The proposed legislation designates the National Cybersecurity and Communications Integration Center (NCCIC) at DHS as the federal "cyber threat indicator portal" to receive and distribute cyber threat indicators in as close to real time as practicable under the circumstances.

AUTHORIZED DISCLOSURES

The legislation authorizes any private entity to disclose *lawfully obtained* cyber threat indicators to the NCCIC, private information sharing and analysis organizations, and federal law enforcement. Entities are required to reasonably limit the disclosure of indicators that contain personally identifiable information or that are otherwise likely to identify specific persons. Entities must also comply with any reasonable restrictions that another entity might place on downstream disclosure of the information.

The proposed legislation also directs DHS to select a private entity to develop a set of best practices for the creation and operation of the aforementioned private information sharing and analysis organizations. One example of a successful regional organization is the Advanced Cyber Security Center.

NO LIABILITY

The legislation provides that private entities are exempt from criminal and civil liability when they voluntarily disclose or receive cyber threat information consistent with the proposed law.

The legislation also ensures that cyber threat indicators shared with the NCCIC are exempt from Freedom of Information Act (FOIA) and state FOIA laws, and may not be used as evidence in a regulatory enforcement action against the disclosing entity.

PRIVACY PROTECTIONS

The proposed legislation directs the attorney general, in coordination with DHS and other federal agencies, to implement policies and procedures governing the receipt, retention, use and disclosure of cyber threat indicators by federal entities. These policies must do the following:

- Reasonably limit the acquisition, interception, retention, use and disclosure of cyber threat indicators reasonably likely to identify specific persons, consistent with the need to carry out the responsibilities of the Breach Notification Act
- Establish a process for timely destruction of information known not to be directly related to a cyber threat
- Establish a process to anonymize and safeguard information
- Protect the confidentiality of proprietary information, among other things

The attorney general must also develop guidelines that will allow the use of cyber threat indicators only for the following enforcement efforts: investigation and combat of computer crimes; investigation of threats of death or serious bodily harm; investigation of serious threats to a minor, including sexual exploitation and threats to physical safety; or investigation of attempts or conspiracies to commit the aforementioned offenses.

CONSTRUCTION AND FEDERAL PREEMPTION

The legislation provides that "nothing in the bill may be construed to limit an entity's authority to share information about potential criminal activity or investigations with law enforcement or interfere with existing sharing relationships between private entities and the government." The bill addresses another concern about information sharing by confirming that "nothing shall be construed to permit price-fixing or market allocation between competitors."

As for preemption, the bill makes clear that it preserves all state laws and requirements except those that restrict or otherwise expressly regulate the retention, use or disclosure of cyber threat indicators by private entities, but only to the extent such state laws contain requirements inconsistent with the bill.

NEXT STEPS

On January 28, 2015, the Senate's Homeland Security and Governmental Affairs Committee held a hearing to move forward with the cybersecurity information sharing legislation. Media outlets report that both sides of the aisle said they are committed to get a bill out of the Committee and passed this year.

Proposed Legislation to Modernize Existing Law Enforcement Provisions

The president's third and final legislative proposal on issues of cybersecurity seeks to provide law enforcement with appropriate tools to investigate, disrupt and prosecute cybercrime. In particular, the administration's proposal contains provisions that would do the following:

- Allow for the prosecution of the sale of botnets
- Criminalize the overseas sale of stolen U.S. financial information, such as credit card and bank account numbers
- Expand federal law enforcement authority to deter the

sale of spyware used to stalk or commit identity theft

- Grant courts the requisite authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity

The proposal also would update the U.S. Racketeering Influenced and Corrupt Organizations Act to apply to cybercrimes, clarify the penalties for computer crimes, and make it easier to prosecute organized criminal groups that engage in computer network and similar attacks. The proposal also seeks to modernize the Computer Fraud and Abuse Act to enhance its effectiveness against attacks on computers and computer networks, including those by insiders, while clarifying that insignificant conduct does not fall within the scope of the statute.

The President's Plan for Safeguarding American Consumers and Families

On January 12, 2015, the White House announced the president's plan for Safeguarding American Consumers and Families. The plan consists of four parts organized around the following objectives:

- Improving consumer confidence by tackling identity theft
- Safeguarding student data in the classroom and online
- Convening the public and private sector to tackle privacy issues
- Promoting innovation by improving confidence online

Improving Consumer Confidence by Tackling Identity Theft

In addition to proposing a national breach reporting law (which is covered in depth later in this article), the White House announced that two banks, JPMorgan Chase and Bank of America, have joined a growing number of companies partnering with FICO to make credit scores available for free to their customers. The White House reports that "[t]hrough this effort over half of all adult Americans with credit scores will now have access to this tool to help spot identity theft, through their banks, card issuers, or lenders."

By improving access to credit reports, consumers can better detect and prevent identity theft and fraud and manage their overall financial health. However, improving access to credit reports does not mean that consumers will understand the benefits of monitoring them. Therefore, in order for this proposal to achieve what it sets out to achieve, the administration and the participating organizations will need to consider the importance of consumer education when rolling out this initiative. For this initiative to have the best chance of success, it will be important to improve consumer education in this area—whether through public service announcements or otherwise—to teach consumers the benefits of accessing, analyzing and addressing issues found in their credit reports.

Safeguarding Student Data in the Classroom and Online

In addition to arming consumers with credit reports so that they can take an active role in monitoring their accounts, another important component of the administration's proposal is improving student privacy. The president points to three initiatives in this area.

ENDORSING THE STUDENT PRIVACY PLEDGE

The president, along with a group of major service providers, endorses and supports the Student Privacy Pledge, an initiative led by the Software and Information Industry Association and the Future of Privacy Forum. This Pledge applies to all student personal information, regardless of how it is collected (via the school or directly through the student's use of an online service), where it is stored (either onsite by the school or offsite by a service provider) or if it is part of an "education record," as defined by federal law. The Pledge asks school service providers to make the following commitments to safeguarding student data:

- Not to collect, maintain, use or share student information beyond the extent authorized for educational purposes or by the parent or student
- Not to sell student personal information
- Not to use or disclose students' information for the purposes of targeting them through behavioral advertising
- To use data for authorized education purposes only

- Not to change privacy policies without notice and choice
- To enforce strict limits on data retention
- To support parental access to, and correction of errors in, children's data
- To maintain a comprehensive security program designed to protect student data from unauthorized access, use or disclosure
- To be transparent about collection and use of data

These commitments are intended to spearhead an industry practice that protects student data beyond what is provided by current law. More than 75 companies have taken the Pledge, and the president encourages more companies to sign on to these commitments. The Pledge is voluntary at this point, but organizations signing on to these commitments should ensure they are able to comply. Where an organization takes the Pledge but fails to honor it, such action could be construed as an "unfair" or "deceptive" act or practice under consumer protection laws and be subject to an enforcement action by the FTC or any state regulator with authority to enforce those laws. Organizations that act as service providers to schools and educators can review the commitments by visiting www.studentprivacypledge.org.

DEPARTMENT OF EDUCATION TOOLS FOR EMPOWERING EDUCATORS

The second component of the president's student privacy initiative is a set of forthcoming tools from the U.S. Department of Education designed to help educators protect student data. The administration reports that these tools will include model terms of service and teacher training assistance that will ensure student data is used appropriately and only according to an educational mission. Schools and other organizations should be able to implement these tools as part of an organization-wide initiative to promote the privacy and security of the student information that is handled and accessed in connection with their work.

THE STUDENT DIGITAL PRIVACY ACT

The third and final part of the White House's plan on student privacy involves a soon-to-be-released legislative proposal for the Student Digital Privacy Act. This Act will seek to ensure that student data collected in an educational context is not sold or used for purposes unrelated to education. It will also encourage research initiatives to improve student learning and support innovation in education technologies that enhance the classroom experience.

The forthcoming legislation is said to be modeled after California's landmark Student Online Personal Information Protection Act (SOPIPA), which will take effect on January 1, 2016. SOPIPA applies to operators of internet websites, online services, mobile applications and mobile services (collectively, online services) that have actual knowledge that these online services are designed, marketed and used primarily for K-12 students. SOPIPA does not apply to general audience websites, such as Google, that are used by K-12 students but not designed for their use specifically.

SOPIPA prohibits operators from the following actions:

- Knowingly engaging in targeted advertising to students or their parents or guardians via online services
- Engaging in targeted advertising via a different online service using any information collected on the operator's online service
- Using information created or gathered from the operator's online service to generate a profile about a student
- Selling a student's information
- Disclosing student information to third parties for a purpose other than a K-12 purpose or a purpose otherwise authorized by the law

SOPIPA also requires operators to maintain reasonable security measures to protect students' information from unauthorized access, destruction, use, modification or disclosure.

Many expect the Student Digital Privacy Act to receive broad bipartisan support. If the law does mirror SOPIPA, an organization's compliance efforts for SOPIPA will likely assist with compliance efforts for the federal act.

Convening the Public and Private Sectors to Tackle Privacy Issues

The next part of the administration's efforts to enhance consumer privacy includes convening the public and private sectors to address emerging privacy issues. This effort includes work done over the past few years by the U.S. Department of Commerce's National Transportation and Information Association to convene multi-stakeholder meetings to establish voluntary codes of conduct addressing mobile application transparency and facial recognition technology.

The latest effort at a voluntary code comes from the U.S. Department of Energy and the Federal Smart Grid Taskforce, which facilitated a multi-stakeholder process to develop a Voluntary Code of Conduct (VCC) for utilities and third parties providing consumer energy use services that would address data privacy related to smart grid technologies. The VCC was designed around five core fair information practice principles (FIPPs). Regardless of whether an organization is governed by the VCC (*i.e.*, engaged in providing consumer energy use services), the VCC can be used as a guide for building a privacy and security program based on the FIPPs. The elements of the VCC are as follows:

- **Customer notice and awareness.** Organizations should send their customers clear and conspicuous notice about privacy-related practices as part of providing service, including
  - The types of data collected
  - The means by which data is collected
  - How data is used and the circumstances under which it is shared with third parties
  - How the customer can access data
  - How the data is secured
  - How data is retained and disposed of
- **Customer choice and consent.** Organizations should allow their customers to choose if and how their data is shared through a process that
  - Explains how a customer can exercise his or her choice
  - Explains specifically which data elements are proposed to be shared
  - Allows customers to authorize and rescind authorization for different types of disclosures
  - Requires consent for disclosure of data for a purpose other than the original purpose for which it was collected
  - Is secure so that customers are reasonably protected against disclosures based on fraudulent consent
  - Ceases disclosure when a customer rescinds authorization, authorization expires or service is terminated
  - Is cost-efficient
  - Allows service providers to charge a fee for non-standard requests

This concept also suggests that businesses retain customer data only as long as needed to fulfill the purpose for which it was collected, and to securely and irreversibly dispose of or de-identify data once the data is no longer needed.

- **Customer data access.** Organizations should grant customers both reasonable access and the ability to maintain their own data through a process that
  - Is reasonably convenient, timely and cost-effective
  - Allows for identification and correction of inaccuracies
  - Allows service providers to charge a fee for accessing data through an unusual method
  - Allows service providers to recover costs for unusual aggregated data requests
- **Data integrity and security.** Organizations should maintain customer data that is as accurate as

reasonably possible and secured against unauthorized access by a cybersecurity risk management program that

- Identifies, analyzes and mitigates security risks
- Implements process, technology and training measures to preserve data integrity and prevent unauthorized use
- Maintains a comprehensive data breach response program
- Provides complete, accurate and timely notices to customers affected by a data breach
- Informs a customer if his or her data has been enhanced or modified from the original form in which it was collected

This concept also sets forth variables (such as customer identifiers, number of customers, timescale and customer class) to consider when aggregating and anonymizing data in a cybersecurity program.

- **Self-enforcement meetings and redress.** Organizations should employ internal enforcement mechanisms to ensure compliance with the VCC principles, including commitments to
  - Regularly review data practices
  - Take action to meet legal and regulatory requirements
  - Provide a simple, efficient and effective means for addressing customer concerns
  - Conduct regular training for relevant employees

On January 12, 2015, the Department of Energy released the VCC with an open invitation for companies to agree to comply. The VCC reflects more than a year of gathering, considering and implementing comments from energy industry stakeholders, privacy experts and the public. Whether the VCC actually gains traction within the energy sector remains to be seen, however, as many companies are still in the process of evaluating its implications.

Promoting Innovation by Improving Confidence Online

The fourth part of the administration's plan includes a renewed call for legislation, and a revamped Consumer Privacy Bill of Rights first released by the White House in its 2012 report Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.

The 2012 report proposed a consumer privacy framework consisting of a Consumer Privacy Bill of Rights built upon a set of FIPPs first promulgated by the U.S. Department of Health, Education and Welfare in the 1970s. This Consumer Privacy Bill of Rights was intended to codify consumer expectations with regard to organizations' use and storage of personal data. While recognizing the responsibilities that consumers have in protecting their own privacy, the Bill of Rights emphasized the importance of businesses using personal data in a manner consistent with the context in which it was collected.

On January 12, 2015, the U.S. Department of Commerce announced that it had completed its public consultation and revision to a draft legislation enshrining the framework into law. This draft is expected to be released toward the end of February 2015.

If a Consumer Privacy Bill of Rights is codified into law, it may facilitate greater ease of data transfer to the European Union and other the global regimes with broader privacy mandates than those currently in place in the United States. However, this portion of the president's proposal is likely the most controversial, because an omnibus privacy law has never enjoyed congressional support. As a result, the administration's continued support for development of self-regulatory frameworks and voluntary codes of compliance based on the FIPPs is likely a more realistic outcome.

Conclusion

President Obama's January 2015 proposals on privacy and cybersecurity demonstrate that the administration wants to take a forward-looking and preventative approach to tackling these issues. Although this approach is commendable, it may prove complicated when trying to

work together with a backward-looking Congress, whose efforts to address these issues seem to ramp up only after there is public outcry or pressure from the administration to get things done. As 2015 progresses, there will likely be movement on the Breach Notification Act, Student Online Privacy Act, and efforts to open communication on cybersecurity between public and private entities. A stalemate, or at least a sizeable debate, seems likely on some of the other more controversial proposals.

THE MCDERMOTT DIFFERENCE

Keep abreast of further developments regarding these legislative proposals by signing up for updates from McDermott's blog www.ofdigitalinterest.com. In particular, we will post further information as soon as the draft Student Digital Privacy Act and the draft Consumer Bill of Rights are released.

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
227 West Monroe Street
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
3811 Turtle Creek Blvd. Suite 500
Dallas , TX 75219
USA
Tel: +1 972 232 3100
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: +49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

ROME
Via A. Ristori, 38
00197 Rome
Italy
Tel: +39 06 462024 1
Fax: +39 06 489062 85

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, D.C.
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

McDermott
Will & Emery

Boston Brussels Chicago Dallas
Düsseldorf Frankfurt Houston London
Los Angeles Miami Milan Munich
New York Orange County Paris Rome
Seoul Silicon Valley Washington, D.C.

Strategic alliance with MWE China Law Offices (Shanghai)

www.mwe.com