Skadden

PRIVACY & CYBERSECURITY UPDATE

JANUARY 14, 2015

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 5, or your regular Skadden contact.

* * *

PRESIDENT ANNOUNCES CYBERSECURITY LEGISLATIVE AND REGULATORY PROPOSALS

On January 12 and 13, in speeches at the Federal Trade Commission (FTC) and the National Cybersecurity and Communications Integration Center (NCCIC), President Barack Obama announced several initiatives to enhance online privacy and cybersecurity. These include (a) several new legislative proposals and (b) new public-private collaborations with the financial, energy and education sectors. Together, these initiatives form a plan that the president is expected to announce in his State of the Union Address. This plan builds upon the president's February 12, 2013, cybersecurity executive order,[1] while acknowledging the limits on the executive branch's ability to address the issue without congressional action.

The president's proposals replicate many of the features of his 2011 cybersecurity legislative initiative,[2] including additional public-private information-sharing authorities, revisions to criminal laws related to computer crimes and a federal data breach notification law. Reports indicate that more recommendations from that proposal, such as additional funding to enhance the cybersecurity workforce, may be announced later this week.

Although the 2011 proposal encountered stiff opposition from business groups, the president's new proposals seek to eliminate some of its more controversial components. For example, the president has abandoned the new cybersecurity regulatory authority permitting the Department of Homeland Security to review and approve critical infrastructure cybersecurity frameworks included in the 2011 proposal. This change is likely to reduce some of the business headwinds by reducing the strong opposition from critical infrastructure industries such as financial services and utilities. Moreover, recent events such as the Sony Pictures data breach and the misappropriation of the U.S. Central Command Twitter and YouTube feeds have demonstrated that private sector data breaches and national security considerations are increasingly intertwined, bolstering the case for a federal role in private sector cybersecurity. Finally, the current governance make-up of a Republican-controlled Congress and Democrat-controlled executive branch would allow both parties to claim credit for advancing cybersecurity legislation, an issue without an obvious partisan valence.

These events, and the cautiously positive response from Congress to the president's proposals, further indicate that, as noted in Skadden's December 2014 *Privacy & Cybersecurity Update*, the logjam in enacting cybersecurity legislation finally may be breaking. As cybersecurity incidents continue to make news, related legislation could be one of the very few areas ripe for bipartisan agreement.

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000

[1] *See* Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, *Privacy & Cybersecurity Update: President Issues Cybersecurity Executive Order*, February 13, 2013.
[2] *See* Letters of Jacob J. Lew, Director of Office of Management and Budget, to The Honorable John Boehner, Speaker of the House of Representatives and the Honorable Joseph Biden, President of the Senate, May 12, 2011 (enclosing president's legislative proposals).

LEGISLATIVE INITIATIVES: REDRAWING THE MAP

The White House has released versions of its proposals both to Congress and to the public.[3] These draft bills can be expected to change as Congress addresses its priorities, tweaks definitions and cleans up inconsistencies. The president's initial plan includes a number of distinct legislative proposals:

- **Information Sharing:** Information-sharing legislation is likely to cause the greatest controversy. For years, the House has tried and failed to have the Senate take up the Cyber Intelligence Sharing and Protection Act (CISPA).[4] CISPA would allow the government to share certain classified intelligence related to cybersecurity threats with private sector entities and allow private sector entities to share threat information with federal agencies or others, notwithstanding any other provision of law. As modified in successive drafts, CISPA and its predecessors have received increasing bipartisan support in the House over the years but have foundered in the Senate over civil liberties concerns and the desire to enact more comprehensive legislation.

  The president's updated cybersecurity information-sharing proposal would encourage private sector entities to share cyber threat information with NCCIC and with private sector-developed and operated Information Sharing and Analysis Organizations (ISAOs).

  Skadden Insights: The president's bill would include significant liability protection, the key issue for many companies interested in sharing information with NCCIC and the ISAOs, which remain concerned about wiretapping, antitrust and other legal implications. In particular, the draft bill would limit civil and criminal liability for sharing information, prohibit regulators from enforcement actions based on voluntarily shared information and exempt shared information from certain provisions of the Freedom of Information Act. Regulators may pursue action based on information shared voluntarily if the same information is uncovered independently from other sources. Notably, the statute requires information that is shared to be "necessary to indicate, describe or identify" the threat in question, and "information that can be used to identify specific persons" must be eliminated before threat information is shared.

  The proposed model is similar, though not identical, to the information-sharing regime in CISPA, though the limits on the information that may be shared are distinct. The burdens involved in identifying cyber threat indicators and personal information likely will determine the degree to which this bill will enhance information sharing. Both are likely to be central to the debates over the civil liberties implications of the president's proposal as well.

- **Data Notification and Protection:** The president's proposal would set a single unified federal standard for post-data breach notification, including a 30-day notification requirement from the discovery of a breach, as well as provisions to further criminalize identity theft. Today, 47 states and the District of Columbia each require that their citizens be notified in the event of certain data breaches. While not every state law is different, there are sufficient variations, including with respect to what events trigger a notice, that the cost of compliance is high. Members of Congress in both parties, the president and various business interests have condemned the status quo, and all have advanced proposals to rectify the problem. A federal data breach law would appear to be a potential point of bipartisan agreement.

  Skadden Insights: The president's proposal largely eliminates states' ability to preempt federal data breach standards, a critical provision for businesses, which have argued that standardization is the key advantage of a federal statute. However, state attorneys general have pushed for additional autonomy to impose more stringent requirements and may continue to do so. For example, the White House proposal requires notification within 30 days of discovery of a data breach, but some states have argued that they should have the right to shorten this period for their own citizens.

---

[3] *See* Letters of Shaun Donovan, Director of Office of Management and Budget, to The Honorable John Boehner, Speaker of the House of Representatives and the Honorable Joseph Biden, President of the Senate, January 13, 2015 (enclosing president's legislative proposals).

[4] H.R. 3523 (2012), H.R. 624 (2013).

States also may seek the right to require notice in situations not covered by the statute. For example, the proposal also provides a safe harbor for those who inadvertently share information but assess the risk and believe there is no reasonable risk of harm to the persons associated with that information (*e.g.*, if the information is encrypted). However, many states still require notification in such circumstances and may push to continue to enforce those provisions. While federal breach notification may be the most likely bill to pass, various competing visions for federal data breach notification will contend in Congress, and the final statute may bear little resemblance to the president's proposal.

- **Law Enforcement Authorities:** The president's updated cybersecurity law enforcement authorities proposal would criminalize a number of activities, including, e.g., the sale of botnets or spyware. The proposal also would update the Racketeering Influenced and Corrupt Organizations Act to apply to cybercrimes. Finally, it would revise the Computer Fraud and Abuse Act (CFAA) to ensure that certain conduct does not fall within the law, while also clarifying that prosecutors may use the statute to pursue company insiders who exceed their authorized access and altering the set of applicable penalties.

  Skadden Insights: Law enforcement has sought updated authorities for many years, and the agencies have strong backing within the House and Senate Judiciary committees, so this proposal may serve as the basis for action. Businesses facing common cybercrimes often find they have little recourse against the criminals in question; such businesses should take note that the CFAA contains a private right of action. Additional CFAA authorities for law enforcement correspondingly will increase the scope of businesses' ability to pursue their rights against those who access their data without authority.

- **Student Digital Privacy:** This bill, reportedly modeled on California's Student Online Personal Information Protection Act, would regulate certain companies that collect student data to prevent them from selling information to third parties for purposes unrelated to the educational mission of their products and services. Students have long argued that they cannot opt out of using vendors who sell their data since schools often mandate the use of specified vendors. This proposal is consistent with the government's sector-specific approach to data privacy regulation. As opposed to the omnibus privacy laws in the EU and certain other countries, the U.S. has opted to protect classes of data, such as health and financial information.[5] Here, again, the president and Congress may find common ground in protecting the information of students, a class of users with a strong political constituency.

  Skadden Insights: This proposal also may find traction, even in a Congress generally averse to regulatory approaches. However, should the sector-specific approach continue to drive federal regulation of the use and collection of data, Congress may create a second patchwork similar to the one it hopes to eliminate with the federal breach notification standard. As data is collected and cross-referenced in a broad array of "big data" applications, it may become increasingly difficult for data collectors to ensure that each piece of data is protected in a manner appropriate to the statute that pertains to the entity by which it was originally collected.

- **Consumer Privacy Bill of Rights:** This bill would develop and apply governing principles for users' expectations of privacy in their online interactions. The text of this legislation is expected to be released by the Commerce Department within 45 days. The president's 2012 framework for such a bill proposed to grant new enforcement authorities to the FTC and state attorneys general to enforce certain online codes of conduct.

  Skadden Insights: Comprehensive privacy regulation has not found a strong constituency in Congress, particularly inasmuch as the FTC's existing efforts in privacy regulation have proven controversial. An overarching privacy bill is the least likely of the president's legislative efforts to succeed.

---

[5] *See, e.g.*, the Electronic Communications Privacy Act with respect to communications-related information, the Health Insurance Portability and Accountability Act of 1996 with respect to health information and the Gramm-Leach-Bliley Act with respect to financial information.

EXECUTIVE ACTION: COLORING IN THE CORNERS

Consistent with the approach taken in the executive order, the president also has announced a number of steps that the government plans to take in concert with the private sector to advance consumer privacy and data security:

- A number of banks and credit unions already have agreed to make credit scores available to consumers for free in order to provide an early warning of potential identity theft.
- Several companies voluntarily have committed to protect students from the misuse of collected information.
- The Department of Education has announced forthcoming model terms of service for use of data collected in educational settings.
- The Department of Energy and the Federal Smart Grid Task Force have released a new voluntary code of conduct (VCC) for utilities and third parties aimed at protecting customer data such as energy usage information.

Collectively, this set of actions demonstrates both the executive branch's power to promote continued private sector action and the limitations on that power. The release of the president's Cybersecurity Framework by the National Institute of Standards and Technology (NIST) has demonstrated that nominally voluntary guidelines for promoting privacy and cybersecurity can become de facto standards. Financial services providers, utilities and others have increasingly used the NIST framework to evaluate their cybersecurity protections, in part because regulators are requesting evidence that such providers have done so. The smart grid VCC appears to be another example of this targeted approach in action – using nominally voluntary guidelines to engage in quasi-regulatory action.

Among providers of software and services to educational institutions, however, the president has taken a full-spectrum approach. While the Department of Education has released a code of conduct for such providers and has collected a number of voluntary adherents to certain general data usage principles, the president is still putting forward the student data privacy protection proposal discussed above. In less-regulated sectors such as education, the president appears to believe that executive action will be correspondingly less persuasive.

Moreover, all of the actions above are sector-specific, demonstrating the piecemeal authority that the executive branch currently possesses to regulate cybersecurity. Without Congressional action, the president will continue to task agencies to solve smaller cybersecurity problems while the larger issues go unaddressed.

Skadden contacts appear on the next page.

SKADDEN CONTACTS

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Jonathan M. Gafni
Counsel / Washington, D.C.
202.371.7273
jonathan.gafni@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com