State Of The Union Sets Stage For Privacy Legislation

Law360, New York (January 21, 2015, 10:15 AM ET) --

President Obama devoted a portion of his 2015 State of the Union address to privacy and cybersecurity, calling for the U.S. Congress to pass comprehensive privacy and cybersecurity legislation in the wake of recent high-profile corporate data breaches, cyberattacks on government agencies, and a growing public interest in how companies collect, store and use consumer data.

In the speech, the president noted the recent alleged state-sponsored cyberattacks that have resulted in compromised corporate networks, theft of trade secrets, and a rise in identity theft, and called for greater intelligence to combat cyberthreats. The president warned that a failure to act poses a threat to the country's economy and security. He called for action designed to protect the technologies, intellectual property, and Internet infrastructure that "have unleashed untold opportunities for people around the globe."[1]

The president used the powerful platform to advocate for new legislation previously outlined during the days leading up to the address. Thus, it is necessary to review the statements made at the Federal Trade Commission, the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center ("NCCIC"), and elsewhere to better understand the president's specific recommendations underlining this new legislation proposal.

On Jan. 12, President Obama announced at the FTC "new proposals on how [the U.S.] can keep seizing the possibilities of an Information Age, while protecting the security and prosperity and values that we all cherish."[2] The president touted his record on privacy by highlighting the FTC's new identity theft hub — IdentityTheft.gov — and the commission's cooperation with credit bureaus to assist identity theft victims. He also noted the government's BuySecure initiative, which aims to secure payments to and from the federal government by implementing chip-and-PIN technology for government credit and debit cards and upgrading retail payment card terminals at federal facilities to accept such cards.

The president announced that he would champion legislation to establish "a single, strong national standard" for data breach notification, requiring companies "to notify consumers of a breach within 30 days." The White House fact sheet published in concert with the speech explains that the proposal would establish "a 30-day notification requirement from the discovery of a breach."[3] The president also voiced an intent to propose ways to "close loopholes in the law" to better prosecute criminals who steal and sell personal data "even when they do it overseas."

The president additionally stated that he hopes to work with Congress to enact a Consumer Privacy Bill of Rights containing basic protections across industries, including the right of consumers to:

1. decide what personal information companies collect from them and how companies use such information;
2. know the purposes for which the information was collected and prohibit its use for a different purpose; and
3. have personal information stored securely.

The president also used the speech to propose the Student Digital Privacy Act, legislation that would prohibit companies from selling student data to third parties for purposes other than education and "prevent any kind of profiling that puts certain students at a disadvantage as they go through school." According to the White House fact sheet, the bill is modeled on California's Student Online Personal Information Protection Act, and includes recommendations of the White House big data and privacy review.[4] The president announced that the U.S. Department of Education and its Privacy Technical Assurance Center will provide educational institutions with new tools to protect student data privacy. These efforts will include model terms of service and teacher training to ensure educational data is used appropriately and consistent with the educational mission.

On Jan. 13, before meeting with congressional leadership, the president again addressed cybersecurity and expressed optimism for bipartisan support for cybersecurity legislation. The president reported consulting with House Speaker John Boehner, R-Ohio, and Senate Majority Leader Mitch McConnell, R-Ky., about the need for cybersecurity to protect critical infrastructure and personal information from cyber threats, and agreeing it is an area both political parties can support with legislation.[5]

On the same day, the president delivered remarks at the NCCIC, calling cyberthreats "one of the most serious economic and national security challenges we face as a nation."[6] The president emphasized the need for cyberthreat information sharing between government and the private sector, noting that much of the nation's critical infrastructure, such as financial systems, power grids, pipelines and health care systems, depend on interconnected network infrastructure owned and operated by the private sector. During that speech, the president announced proposed legislation to promote greater information sharing between the government and the private sector that will include liability protections for companies that share information on cyberthreats. The legislation will also include safeguards to ensure that the government protects privacy and civil liberties.

According to the White House press release companying the speech, the president's legislative proposal will be designed to encourage the private sector to share appropriate cyberthreat information with the Department of Homeland Security's National Cybersecurity and Communications Integration Center, which will in turn share the information in real time as practicable with other federal agencies and with private sector-developed and operated Information Sharing and Analysis Centers (ISACs).[7] In response to the concerns about privacy and civil liberties, the proposal would require "private entities to comply with certain privacy restrictions such as removing unnecessary personal information and taking measure to protect any personal information that must be shared in order to qualify for liability protection. The proposal further requires the Department of Homeland Security and the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board and others, to develop receipt,

retention, use, and disclosure guidelines for the federal government."

The president also proposed updates to law enforcement's authority to pursue and prosecute cybercriminals. According to the White House press release, the legislation will:

1. allow for the prosecution of the sale of botnets;
2. criminalize the overseas sale of stolen U.S. financial information, such as credit card and bank account numbers;
3. expand federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft; and
4. empower courts with the authority to shut down botnets engaged in distributed denial of service attacks and other cybercriminal activity.

The proposal also would amend the Computer Fraud and Abuse Act to exclude insignificant conduct, "while making clear that it can be used to prosecute insiders who abuse their ability to access information to use it for their own purposes."

The president stated that the White House will convene a cybersecurity summit at Stanford University on Feb. 13 to bring together government officials, industry leaders, and academics to address a range of issues. The White House press release lists current topics for the summit, including "increasing public-private partnerships and cybersecurity information sharing, creating and promoting improved cybersecurity practices and technologies, and improving adoption and use of more secure payment technologies."

On Jan. 15, Vice President Biden announced that over the next five years, the U.S. Department of Energy will provide $25 million in grants from the Minority Serving Institutions Partnership Program of the National Nuclear Security Administration to support a Cybersecurity Workforce Pipeline Consortium consisting of 13 historically black colleges and universities, two Department of Energy laboratories, and the Charleston County School District. According to the White House press release, the "Program focuses on building a strong pipeline of talent from minority-serving institutions to DOE labs, with a mix of research collaborations, involvement of DOE scientists in mentoring, teaching and curriculum development, and direct recruitment of students."[8]

Lastly, on Jan. 16, President Obama and U.K. Prime Minister David Cameron announced that the United States and United Kingdom have agreed on several initiatives to strengthen cybersecurity cooperation between the two countries. According to the White House press release, "both governments have agreed to bolster our efforts to increase threat information sharing and conduct joint cybersecurity and network defense exercises to enhance our combined ability to respond to malicious cyber activity."[9] These efforts will focus on protecting critical infrastructure, and the first joint defense exercise will concentrate on the financial sector.

In addition, the two leaders announced the creation of a joint cyber cell to "focus on specific cyber defense topics and enable cyber threat information and data to be shared at pace and at greater scale." The cyber cell will have a presence in each country and will be staffed by the United Kingdom's Government Communications Headquarters and Security Service (MI5), and

the United States' National Security Agency and Federal Bureau of Investigation. The joint statement also announced that the two governments will fund a Fulbright Cyber Security Award to enable scholars to conduct cybersecurity research for up to six months.

The State of the Union address may mark a new phase in the political discourse concerning privacy and cybersecurity. Attention from Washington has never been greater. Increased attention, however, likely brings an increase in industry debate and partisan opposition. In promoting a single, national standard for consumer notification of data breaches, for example, the president has emphasized the costs borne by companies that currently must comply with over 50 state and territorial notification statutes in the United States. Some industry voices agree. Others, however, will likely take issue with the proposed statute's rigid 30-day notification requirement. Likewise, companies that may otherwise participate in the proposed information sharing program will likely require more details concerning the "targeted liability protection" promised by the president. And the renewed proposal for a Consumer Privacy Bill of Rights will awaken old debates about the proper use of consumer data.

The high-profile data breaches perpetrated against familiar companies brought cybersecurity concerns into homes across America and set the stage for new legislative and executive efforts. Whether those efforts will yield tangible results without an attendant increase in corporate liability remains to be seen.

—By Mauricio Paez, Todd McClelland, Jay Johnson and Gabe Ledeen, Jones Day

Mauricio Paez is a partner in Jones Day's New York office. Todd McClelland is a partner in the firm's Atlanta office. Jay Johnson is of counsel in the firm's Dallas office. Gabe Ledeen is an associate in the firm's San Francisco office.

[1] President Obama's State of the Union Address—Remarks as Prepared for Delivery, available at https://medium.com/@WhiteHouse/president-obamas-state-of-the-union-address-remarks-as-prepared-for-delivery-55f9825449b2.

[2] Remarks by the President at the Federal Trade Commission, available at http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

[3] FACT SHEET: Safeguarding American Consumers & Families, available at http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

[4] See Big Data: Seizing Opportunities, Preserving Values, available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.p

df.

[5] Remarks by the President Before Meeting with Congressional Leadership, available at http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-meeting-congressional-leadership.

[6] Remarks by the President at the National Cybersecurity Communications Integration Center, available at http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.

[7] SECURING CYBERSPACE – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts, available at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[8] Vice President Biden Announces $25 Million in Funding for Cybersecurity Education at HBCUs, available at http://www.whitehouse.gov/the-press-office/2015/01/15/vice-president-biden-announces-25-million-funding-cybersecurity-educatio.

[9] FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation, available at http://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.