Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 1 >>> JANUARY 2015

U.S. President Obama Announces Renewed Focus on Securing Cyberspace and Protecting Consumer Privacy

By Alexander H. Southwell, Eric D. Vandevelde, Ryan T. Bergsieker, Stephenie Gosnell Handler and Adam Chen, of Gibson, Dunn & Crutcher LLP.

In the days leading up to his State of the Union address scheduled for January 20, 2015, President Obama outlined several significant cybersecurity and data privacy initiatives.

This renewed focus on cybersecurity comes in the wake of a number of prominent cyber attacks on U.S. companies in recent months that have captured national and international attention, and includes both proposed legislation and executive actions.

Several of the initiatives seek to protect American consumers from cyber threats while ensuring privacy and civil liberties.

They mark an evolution in the Administration's approach to cybersecurity and come after years of stalled efforts to pass cybersecurity legislation. Their unveiling establishes cybersecurity and data privacy as focal points of the president's upcoming State of the Union address and reinvigorated priorities for the Administration.

While politics will shape the final version of these proposals, this article examines, from a legal perspective, the initiatives as an outline of the Administration's goals in cybersecurity and data privacy.

Proposed Cybersecurity Legislation

President Obama officially announced proposed cybersecurity legislation in a speech on January 13, 2015, at the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). The legislative proposal consists primarily of cybersecurity information sharing and law enforcement tools.

Cybersecurity Information Sharing

The proposed legislation would promote enhanced cybersecurity information sharing between the private sector and the government, and seek to increase collaboration and information sharing in the private sector.

The NCCIC would play a significant role under the proposal, as it would be tasked with sharing cyber threat information received from the private sector (*e.g.*, Internet protocol (IP) addresses and other routing information associated with malicious actors) with relevant federal agencies and other private sector organizations that have been established for the purpose of

information sharing and analysis, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The proposed legislation is intended to reinforce and strengthen existing relationships between the federal government and the private sector. It also would encourage the development of additional private sector-led information sharing and analysis organizations like FS-ISAC, which is highly regarded for facilitating anonymous information sharing and analysis within the financial services industry.

Importantly, the proposed legislation would provide "targeted" liability protection for companies that share information. In an attempt to accommodate privacy concerns, the proposal stipulates that, in order to qualify for such liability protection, companies would be required to "remov[e] unnecessary personal information and tak[e] measures to protect any personal information that must be shared." The White House thus far has not clarified how this requirement would be implemented.

While the proposed liability protection appears intended to be narrower than previous initiatives, privacy advocates will undoubtedly express concerns.

Further, the proposed legislation would require the development of guidelines regarding the receipt, retention, use, and disclosure of data maintained by the federal government. The Department of Homeland Security and the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board, would be responsible for developing such guidelines.

Prosecuting Cyber Crime

The proposed legislation also would include provisions aimed at enhancing the investigation, deterrence, and prosecution of cyber crimes.

Specifically, the legislation would:

- facilitate prosecution of the sale of botnets;
- criminalize foreign sales of stolen U.S. personal financial information (*e.g.*, credit card and bank account numbers);
- expand federal law enforcement authority to deter the sale of spyware used to stalk or commit identity theft; and
- authorize courts to shut down botnets engaged in distributed denial of service attacks and other criminal activity.

Further, the proposed legislation would revise certain existing criminal laws.

The Computer Fraud and Abuse Act (CFAA) would be amended to allow the prosecution of "insiders" (*e.g.*, employees) who abuse their computer or network access rights to engage in significant malicious conduct. This would resolve a split in the federal circuit courts created by the Ninth Circuit, which has held that violating contract-based restrictions (*e.g.*, terms of service and corporate computer use policies), as opposed to circumventing code-based or technological restrictions, cannot constitute unauthorized access. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc)* (limiting application of the CFAA's "exceeds authorized access" prong to "circumvention of technological access barriers").

The Racketeer Influenced and Corrupt Organizations (RICO) Act also would be revised to explicitly apply to cyber crimes and to clarify penalties for such crimes, aligning them with penalties for comparable non-cyber crimes.

Data Privacy and Consumer Protections

President Obama also proposed several pieces of online consumer protection and data privacy legislation in a speech at the Federal Trade Commission (FTC) on January 12, 2015. The proposals build upon the Administration's recent efforts in the consumer privacy and identity theft realm and seek to protect American consumers from cyber threats.

Personal Data Notification and Protection Act

President Obama's proposal would set forth a new legislative regime federalizing data breach notification by covering consumers whose personal and financial information has been compromised in a data breach and who are at risk of identity theft—an initiative the White House and many in Congress have supported for years.

While the text of the proposed bill has yet to be released, the Personal Data Notification and Protection Act (PDNPA) would, among other things, clarify and strengthen the obligations companies have to notify customers when their personal information has been exposed in a data breach, and seek to preempt the existing patchwork of 47 state data breach notification laws with a single national standard. The PDNPA would require companies to notify consumers within 30 days from the discovery of a breach.

This requirement stands in contrast to many state laws that currently require notification without unreasonable delay, but with no statutory deadline. *See, e.g.*, Ariz. Rev. Stat. Tit. 44, Ch. 32, 44-7501 ("The notice shall be made in the most expedient manner possible and without unreasonable delay."); Cal. Civ. Code § 1798.29 ("The disclosure shall be made in the most expedient time possible and without unreasonable delay."); Del. C., Tit. 6, Chapter 12B, § 102 ("Notice must be made in the most expedient time possible and without unreasonable delay."); 815 Ill. Comp. Stat. 530/10 ("The disclosure notification shall be made in the most expedient time possible and without unreasonable delay.").

The PDNPA would simplify notification requirements and potentially lower compliance costs by allowing companies to focus their compliance regime on one standard instead of a mishmash of laws.

However, the PDNPA could afford companies less discretion in deciding when and how to notify consumers, which would underscore the need for companies to develop robust response plans in advance of any cyber in-

   ISSN 1473-3579

cident, to allow them to provide notifications to consumers within the required timeframe.

Consumer Privacy Bill of Rights

The president also announced that the Administration is revitalizing the Consumer Privacy Bill of Rights (CPBR), previously proposed in 2012.

The new CPBR will attempt to set clear principles regarding the context in which personal data can be collected online, and seek to ensure that consumers' expectations regarding the use of such data are not abused. The proposed legislation would grant consumers the right to decide what personal data companies can collect and how such data is used, prohibit unauthorized cross-purpose collection of data (*i.e.*, information collected for one purpose cannot be used for a different purpose), and require companies to store consumers' personal information in a secure manner.

The president's announcement did not include any specific legislative proposal; that proposal is scheduled to be released within 45 days of the announcement and will be closely scrutinized.

Student Digital Privacy Act

The proposed Student Digital Privacy Act (SDPA) would seek to ensure that data collected in the educational context is used only for educational purposes.

The measure would prohibit companies from selling student data to third parties for non-educational purposes and from using such data to engage in targeted student advertising.

It is modeled on California's Student Online Personal Information Protection Act (SOPIPA). SOPIPA prohibits online educational services from amassing student profiles for non-educational purposes, and requires online service providers to maintain adequate security procedures and to delete student information at the request of a school or district. *See* Cal. Bus. & Prof. §§ 22584(b)(2), (d)(1) and (d)(2).

The Administration has not specified whether SDPA will contain similar provisions.

Smart Grid Customer Data Privacy

In addition to these pieces of proposed legislation, the Administration announced that the Department of Energy and the Federal Smart Grid Task Force have released a new Voluntary Code of Conduct for utilities and third parties regarding protecting electricity customer data, including customer energy usage.

Additional White House Initiatives

Finally, the White House announced two additional cybersecurity-related initiatives.

First, on February 13, 2015, the White House will host a Summit on Cybersecurity and Consumer Protection at Stanford University, building on the BuySecure Initiative launched by the president in November 2014. The Summit is intended to bring together key stakeholders from the federal government, the private sector, and law enforcement, as well as privacy advocates, to discuss increasing public-private partnerships, cybersecurity information sharing, and the development and promotion of cybersecurity best practices and technologies.

Second, in recognition of the importance of developing a skilled cybersecurity workforce, the Department of Energy will provide $25 million in grants to support a cybersecurity education consortium that consists of more than a dozen historically black colleges and universities and two national laboratories.

Conclusion

The magnitude of recent cyber attacks on American businesses has heightened the executive branch's sense of urgency around developing comprehensive measures to bolster the nation's abilities to deter, respond to, and recover from cyber attacks.

The recent announcements indicate that the Administration is keenly focused on leading cybersecurity efforts that will facilitate these goals and build upon its previous efforts to set federal standards for consumer privacy and data protection.

It seems likely that 2015 will be a critical year in the development of a more comprehensive federal response to cyber threats.

The text of President Obama's January 13, 2015, speech at the NCCIC can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.

The text of the White House's January 13, 2015, statement "SECURING CYBERSPACE — President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts" can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

The text of President Obama's January 12, 2015, speech at the FTC can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

The text of the White House's January 12, 2015, fact sheet "Safeguarding American Consumers & Families" can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

Alexander H. Southwell is Co-Chair of Gibson, Dunn & Crutcher LLP's Information Technology and Data Privacy Practice Group, and a Partner in the firm's New York office. Eric D. Vandevelde is a Litigation of Counsel in the firm's Los Angeles office. Ryan T. Bergsieker is a Litigation of Counsel in the firm's Denver office. Stephenie Gosnell Handler is a Corporate Associate in the firm's Washington office. Adam Chen is a Litigation Associate in the firm's New York office. The authors may be contacted at asouthwell@gibsondunn.com, evandevelde@gibsondunn.com, rbergsieker@gibsondunn.com, shandler@gibsondunn.com and achen@gibsondunn.com.