crowell moring

CLIENT ALERT

President Obama Announces Major Cyber and Privacy Legislation

Jan.14.2015

On January 13, 2015, President Obama announced several legislative proposals to increase cyber threat information sharing, to create a consistent national data breach notification law, and to modernize cybercrime enforcement. Additional Executive Action is also expected over the next few months. Immediate reactions to the proposed legislation have been mixed, but if all three proposals are enacted, a significant change to existing U.S. privacy and cybersecurity law is expected.

Cybersecurity Information Sharing

The first proposal would enhance cybersecurity information sharing opportunities, both between private sector and the government and among private sector companies, by encouraging formation of Information Sharing and Analysis Organizations (ISAOs). ISAOs, like Information Sharing and Analysis Centers (ISACs), provide mechanisms for companies to share information about cyber threats and vulnerabilities in order to minimize the likelihood and effectiveness of cyber attacks. Additionally, private sector companies that provide "cyber threat indicator" information to the Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) will be shielded from any potential liability resulting from disclosing that information. NCCIC, in turn, will share that information with relevant federal agencies and ISAOs. Key aspects of the proposed law include:

- **Liability Protection**: The law prohibits all civil and criminal causes of action (in any Federal or State court) based on the voluntary disclosure of cyber threat indicators to NCCIC or to a certified ISAO. In addition, no Federal entity may use information disclosed under the law as evidence in a regulatory enforcement action against the entity that disclosed the information.
- **Privacy Concerns**: As the White House press release explained, the proposal requires companies to implement certain privacy and security protections for the information shared with the government and ISAOs in order to qualify for liability protection. In addition, DHS and the Attorney General, working with the Privacy and Civil Liberties Oversight Board (PCLOB), will establish use, retention, and disclosure guidelines for any shared information that, among other things, must:
    - reasonably limit the acquisition, interception, retention, use and disclosure of cyber threat indicators likely to identify specific individuals;
    - establish a process for timely destruction of information that is not directly related to a cyber threat;
    - establish public guidelines that limit government use of disclosed data;
    - penalize any government employee that violates the law;
    - establish a process to anonymize and safeguard information; and
    - protect the confidentiality of proprietary information
- **Preemption**: The law preempts contrary state laws regulating the retention, use, or disclosure of cyber threat indicators by private entities, but contains numerous exceptions the will leave many existing laws in place.

National Data Breach Notification Law

Second, the President proposed a national data breach notification law to harmonize the 47 state breach notification laws (plus D.C. and several territories) that currently exist. Key aspects of the proposed law include:

- **"Sensitive Personally Identifiable Information" (SPII) Definition**: The information types that trigger notification obligations are generally broader than most states and include elements such as: (1) name plus two of the following: home address, telephone number, mother's maiden name, or date of birth; and (2) stand-alone data elements such as a social security number, driver's license number, passport number, other government-issued identification number, biometric data, unique account identifier, or user name or email address with a required password or security code. Other data elements can also trigger notification and the Federal Trade Commission (FTC) will have modified rulemaking authority to alter the definition.
- **Notification Timeline/Applicability**: Companies that handle larger amounts of data (i.e., records about more than 10,000 individuals) must notify individuals of any breach of "personal information" within 30 days. Other than narrow time limits for health facilities in California and for insurers in Connecticut (both 5 days), the proposed law sets a more restrictive notification deadline than any other state (except Florida, which also requires 30 days). Arguably, the law's limited application to companies handling larger amounts of data will leave a wide range of companies outside the scope of the proposed legislation.
- **Harm Trigger/Safe Harbor**: The law requires notifying individuals "unless there is no reasonable risk of harm or fraud to such individual." In order to determine that notification is not warranted under the law, companies must prepare a written assessment of the risk which must be provided to the FTC within 30 days in order to invoke the "safe harbor" protection.
- **Enforcement**: The FTC will enforce violations of the law as unfair and deceptive trade practices. Unless the FTC has already commenced an action, States may also enforce the law (and impose penalties up to $1,000 per person per day, subject to a $1 million max). States must notify the FTC before commencing an enforcement action and the FTC can take charge of any such action.
- **Preemption/Exemption**: The proposed law preempts all other State laws. Covered Entities and Business Associates regulated by the Health Insurance Portability and Accountability Act (HIPAA), as well as personal health records vendors subject to the HITECH Act, are exempt from the proposed law.

Modernization of Cybercrime Laws

Finally, the proposal modernizes cybercrime laws by prosecuting the sale of botnets, criminalizing the overseas sale of stolen U.S. financial information, expanding federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft, and giving courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity. In addition, the proposal clarifies that the existing Racketeering Influenced and Corrupt Organizations Act (RICO) applies equally to cybercrimes. Finally, the proposal modernizes the Computer Fraud and Abuse Act (CFAA) by targeting more serious computer crimes.

Conclusion

There is uncertainty regarding which, if any, of these laws will pass Congress (and what changes will be made to any laws that do pass). However, these laws illustrate the significant priority that the Executive Branch has placed on privacy and cybersecurity. Additional Executive Action is expected over the next several months. We will provide additional updates as they develop.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com