MINTZ

White House Proposes National Data Breach Notification Standard

January 14, 2015 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Written by Cynthia Larose, CIPP and Ari Moskowitz, CIPP

This has been a big week for cybersecurity announcements from Washington. In what the White House has called a series of "SOTU Spoilers," President Obama announced his intention to follow through on some of the recommendations in his administration's **Big Data report** -- the culmination of the White House's 90-day "Big Data" review in 2014. Specifically, the President proposed following through on the report's recommendations that the following legislation be passed: a consumer privacy bill of rights, a national data breach notification law, and a law to promote student privacy.

Speaking at the Federal Trade Commission, the President previewed the **Personal Data Notification & Protection Act**, which would establish a 30-day notification requirement of a data breach while requiring notice by mail, telephone, or if certain conditions are met, email or the media. State laws would mostly be preempted, however, states would still have the authority to require additional information in notices concerning state-specific "victim assistance." Notice to credit to reporting agencies within 30 days, and prior to notice to individuals if possible, would also be required. The White House proposal for a national data breach notification standard would replace the by-now familiar "crazy quilt" of state data breach notification requirements -- **see the Mintz Matrix** in case you need convincing.

The Federal Trade Commission would enforce the law, with violations constituting an unfair or deceptive practice, and the FTC would be given broad rule making authority to issue whatever regulations it seems necessary to carry out its duties with respect to the law. The proposed legislation would require that the FTC coordinate with other agencies in the issuance of regulations when such regulations would affect entities subject to regulation by the Federal Communications Commission or the Consumer Financial Protection Bureau. State Attorneys General would also have the authority to enforce the law, subject to certain FTC rights to intervene, stay, or remove the proceeding. The proposed law does not create, or make any mention of, a private right of action.

The proposed law allows responsibility for notification to be allocated by contract as between the owner of the data and a licensee or other party, and also states that if the data owner provides notification of a breach, third parties that otherwise handle, but do not own, the data, are relieved from any notification requirements. A licensee or other third party that transmits or otherwise handles the "sensitive personally identifiable information" would be required (as under most state laws) to notify the owner of the data in the event that the third party discovers the breach.

The White House proposal contains several exemptions, including a so-called "safe harbor" if the business conducts a risk assessment that determines there would be no reasonable risk of harm to individuals as a result of the breach. Such risk assessment must be conducted -- and the results provided to the FTC -- within the same 30-day "shot clock" period of breach discovery. Other exemptions include delay for law enforcement (Federal only) and if a business participates in certain security programs to prevent financial fraud.

This latest bid for a national data breach notification standard contains many of the provisions that are found in data breach notification laws in the 47 state laws currently on the books and in the 33 proposals introduced in Congress over the last 5 years.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.