Foster Garvey

Washington's Latest Efforts on Data Security and Privacy

Legal Alert
June 11, 2019

Contact

Benjamin J. Hodges

Related Services

IP & Technology

Privacy, Cybersecurity & Data Protection

WASHINGTON STRENGTHENS DATA BREACH LAW, EFFECTIVE MARCH 1, 2020

On May 7, 2019, Governor Jay Inslee signed new legislation strengthening Washington's data breach law, RCW §§ 19.225.010, *et. seq.* The new provisions expand consumer data breach notification requirements to include more types of consumer information and shorten the deadline for businesses to notify consumers and the state attorney general of a breach. The new legislation—which unanimously passed both chambers of the Washington legislature in April 2019—will take effect on March 1, 2020.

EXPANDED BREACH NOTIFICATION REQUIREMENTS INCLUDE MORE TYPES OF "PERSONALLY IDENTIFIABLE INFORMATION"

Under the current law, a business that experiences a data breach must notify consumers only if the breach exposes a consumer's name alongside one of four types of "personally identifiable information": his or her Social Security number, driver's license number, state ID number, or financial account information. The revised law expands this list of "personally identifiable information" to also trigger a business' notification obligations when a consumer's name is exposed in combination with any of the following:

- Full date of birth
- Health insurance ID numbers
- Medical history information
- Student ID numbers
- Military ID numbers
- Passport ID numbers
- Online login credentials, such as username-password combinations or security questions and answers

- Biometric data, such as DNA profiles, fingerprints, voiceprints, or eye retinas
- Electronic signatures

SHORTENED DEADLINE FOR NOTIFYING CONSUMERS OF A BREACH

The new legislation shortens the deadline for notifying affected consumers and the state attorney general of a breach from 45 days to 30 days after discovery.

ADDITIONAL NOTICE REQUIREMENTS

The notice to consumers must now include the "time frame of exposure, if known," including the date the breach occurred and the date of discovery. In addition, the notice to the attorney general—which is mandatory in the event that a single breach affects more than 500 Washington residents—must now include (1) the time frame of exposure; (2) a list of the types of personal information affected by the breach; (3) a summary of the steps taken to contain the breach; and (4) a sample of the notice to be provided to consumers. The law also imposes an ongoing duty to provide updates if any of the required information is not known at the time of notification.

SPECIFIC PROCEDURES FOR COMPROMISED LOGIN CREDENTIALS

Finally, if a breach compromises login credentials — usernames, passwords, or security questions and answers — the new legislation requires that the notice to affected consumers prompt them to take appropriate steps to secure the affected account and all other accounts that use the same credentials. In addition, the law specifies that the company cannot notify consumers of the breach by emailing the compromised account. Instead, the company must employ an alternate notification method, such as posting an alert on its website or contacting the news media.

As the revisions to the data breach law do not take effect until March 1, 2020, Washington businesses have some time to prepare for the coming changes. If you have any questions about how the expanded data breach law might affect you or your business, please contact a member of Foster Pepper's Intellectual Property Team and Foster Pepper's Privacy, Cybersecurity and Data Protection Group.

WASHINGTON LEGISLATURE FAILS TO ENACT DATA PRIVACY BILL

While the changes to the data breach law sailed through both chambers of the Washington state legislature, efforts to enact new statewide privacy regulations stalled in the House of Representatives as legislators, privacy advocates, and key tech players failed to reach an agreement.

The Washington Privacy Act ("WPA"), SB 5376, was modeled after the EU's stringent General Data Protection Regulation ("GDPR") rather than the California Consumer Privacy Act passed last June. The WPA's proposed GDPR-like protections would have made it one of the strongest privacy laws in the country, providing Washington residents with the right to access data that companies have about them in order to ascertain who is using that data and why, the right to correct inaccurate information, the right to delete certain personal data, and the right to opt out of certain uses of data, such as for targeted advertising. The legislation also would have

required companies to take certain steps to prevent data breaches and imposed stricter limitations on the use of facial recognition technology by private businesses and law enforcement.

Although the bill failed to come to a vote in the House this session, with it is 46-1 passage through the Senate, it is likely to be considered again in future sessions.