Updates
January 30, 2019
Proposed Washington Privacy Act Tracks GDPR and CCPA Protections and Emphasizes Facial Recognition

Washington state has joined the growing ranks of states considering data privacy legislation in the wake of the European General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Senate Bill 5376, introduced by Senator Reuven Carlyle (D-Seattle) on January 18, 2019, and known as the Washington Privacy Act (Act), proposes new rights to consumers and restrictions on companies' use of personal data for profiling and facial recognition.

Who would be covered by the Washington Privacy Act?

The Act would apply to legal entities that conduct business in Washington or provide products or services targeted at Washington residents *and* either (1) control or process the personal data of 100,000 or more Washington residents ("consumers") *or* (2) derive more than 50 percent of gross revenue from the sale of personal data and control or process the data of 25,000 or more consumers. The Act expressly excludes individuals acting in their role as employees from protection under the Act, so none of the consumer rights or business obligations described below apply to employee personal data. There are also exemptions for certain medical and financial data to the extent regulated by federal law.

How is personal data defined?

Personal data is succinctly defined as "any information relating to an identified or identifiable natural person." The term does not extend to data that is linked or linkable to devices or households, and de-identified data is specifically carved out.

What rights would consumers have?

Like the GDPR and the CCPA, the Washington Privacy Act would provide consumers with new rights with respect to their personal data, including those of **access**, **portability** (for example, consumers may require businesses to transmit their personal data to other businesses), **correction**, **deletion**, **restricted processing** (for example, where the accuracy of the data is contested by the consumer) and **objection to processing**. Some rights are only available under certain circumstances.

The Act would also require businesses to publish a privacy notice informing consumers of the categories of personal data the business collects and the purposes for which the data is used or disclosed, which mirrors a similar requirement in the CCPA. Additionally, businesses would also be required to inform consumers, at the time of sale or processing, when their personal data is sold to data brokers or processed for direct marketing. Similar to requirements under the GDPR, the Act would also require businesses that engage in profiling to also disclose such profiling at or before the collection of personal data and prohibit them from subjecting consumers to a decision based solely on profiling which produces legal, or similarly significant, effects concerning the consumer (such as the denial of housing, employment opportunities or healthcare services).

What other obligations would businesses have?

In addition to honoring consumers' requests to exercise their rights under the law, businesses would have to conduct and document risk assessments (1) prior to processing personal data, (2) any time processing changes will impact individual consumer risk, and (3) at least once annually. These risk assessments would need to identify and weigh the benefits of processing against the personal risk to the consumer. If the risk outweighed benefit, businesses could not process the data without consumer consent.

What requirements would be imposed regarding facial recognition?

The Washington Privacy Act would impose unique, new obligations on businesses that use facial recognition. These obligations would exceed those obligations already in place under Washington's Biometric Privacy Law (RCW 19.375). Under the proposed law, businesses that use facial recognition for profiling would be required to employ meaningful human review prior to making final decisions based on profiling, if the decisions produced legal or similarly significant effects. Additionally, businesses that use facial recognition on their own behalf (as opposed to those that provide the technology for others to use) would be required to obtain consumer consent prior to deploying facial recognition services. The consent requirement could be met in some circumstances where a consumer enters physical premises with prominent notice that facial recognition is being used.

The Act would also impose requirements on businesses that provide facial recognition technology for others' use, including requiring such businesses to prohibit by contract using facial recognition for discriminatory purposes, to provide documentation about how the technology works, and in certain circumstances, to provide APIs or other technical capability for third parties to test for bias and the accuracy of the facial recognition services. Finally, the Act would prohibit state and local governments from using facial recognition technology for ongoing surveillance of specified individuals in public spaces, with exceptions for certain law enforcement purposes.

What are the potential penalties for violations of the Act?

A violation of the Washington Privacy Act would be considered a violation of Washington's Consumer Protection Act with penalties of up to $2,500 per violation or $7,500 per intentional violation. There is no private right of action under the bill, and the Office of the Attorney General would be responsible for enforcement.

How are Washington stakeholders responding?

On January 22, 2019, the Senate Bill 5376 had a public hearing before the Senate Environment, Energy, and Technology Committee. Although most witnesses agreed with the need for greater privacy protection, some members of the public expressed concern for the compliance burden on small and mid-sized businesses, and others pushed for exemptions based on overlapping compliance obligations in federal privacy statutes, such as the Fair Credit Reporting Act. Based on feedback from the hearing and further advocacy to legislators, the bill will likely undergo amendment as it moves through the legislature.

What should businesses do now?

The bill has not yet passed the Washington state legislature and, if it does, it will likely be effective on December 31, 2020, at the earliest. However, companies can, and should, proactively consider their data hygiene as states increasingly seek to legislate how companies use personal information and there have been a variety of proposals for a new federal privacy law. The following best practices are both helpful for CCPA and GDPR compliance

and can help businesses prepare for the possibility of a new Washington law:

- Systematically assess current privacy practices. Consider conducting a privacy assessment and a mapping exercise to understand how personal data is collected, used, stored, secured and disclosed by the company.
- Review user-facing disclosures, such as website privacy policies, terms and consent flows, to better position the company for compliance.
- Consider how the business will accommodate requests by consumers to exercise rights of access, correction and deletion, as these are new rights that the Washington Privacy Act would afford them.
- Examine whether the company's use of personal data amounts to profiling which produces a legal or similarly significant effect on consumers, in which case consider whether there are exemptions under the that would apply or non-profiling approaches that the company can use to augment its decision-making.
- If the company uses facial recognition, consider options for providing notice and, if appropriate, consent and other public documentation about how the technology works. Confirm that the company is in compliance with existing biometric laws, such as those in Illinois, Texas and Washington.
- Start thinking about how the company would perform the required risk assessment.
- Implement robust, comprehensive data security practices.

For assistance evaluating how to tailor privacy practices to existing and upcoming legislation, please contact experienced counsel. Those wishing to submit feedback on the legislation may provide online comment, contact their legislators, subscribe to email updates or monitor the calendar for future public committee hearings.

© 2019 Perkins Coie LLP

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Interactive Entertainment

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law