Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

2SSB 5376

Brief Description: Protecting consumer data.

Sponsors: Senate Committee on Ways & Means (originally sponsored by Senators Carlyle, Palumbo, Wellman, Mullet, Pedersen, Billig, Hunt, Liias, Rolfes, Saldaña, Hasegawa and Keiser).

Brief Summary of Second Substitute Bill

- Defines obligations for controllers and processors of personal data who are legal entities that meet specified thresholds.
- Exempts state and local government, municipal corporations, and certain entities and data sets from the obligations set forth in the act.
- Requires controllers to facilitate consumer requests to exercise certain rights regarding processing of personal information.
- Makes a violation of the act enforceable only by the Attorney General under the Consumer Protection Act and subject to civil penalties.
- Requires controllers using facial recognition for profiling to meet certain requirements.
- Prohibits the use of facial recognition technology by all state and local government agencies to engage in ongoing surveillance except in specified situations.
- Directs the Office of Privacy and Data Protection to conduct an analysis on the public sector use of facial recognition technology and to report its findings to the Legislature.

Hearing Date: 3/22/19

Staff: Yelena Baker (786-7301).

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Background:

Personal information and privacy interests are protected under various provisions of state law. The Washington State Constitution provides that no person shall be disturbed in his private affairs without authority of law. The Public Records Act protects a person's right to privacy under certain circumstances if disclosure of personal information would be highly offensive and is not of legitimate concern to the public.

The Consumer Protection Act (CPA) prohibits unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General may investigate and prosecute claims under the CPA on behalf of the state or individuals in the state.

In 2016 the Office of Privacy and Data Protection (OPDP) was created to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection. The primary duties of the OPDP with respect to state agencies include conducting privacy reviews and trainings, coordinating data protection, and articulating privacy principles and best policies.

Summary of Bill:

Key Definitions.

"Controller" means the natural or legal person which, along or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" means a natural or legal person that processes personal data on behalf of the controller.

"Consumer" means a natural person who is a Washington resident acting only in an individual or household context and does not include a natural person acting in a commercial or employment context.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person and does not include deindentified data or publicly available information.

"Business purpose" means the processing of personal data for the controller's or its processor's operational purposes, or other notified purposes, provided that the processing of personal data must be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected.

Controller and Processor Obligations.

Specific obligations related to personal data are created for legal entities that conduct business in Washington or intentionally target their products or services to Washington residents and:

- control or process data of at least 100,000 consumers; or

- derive at least 50 percent of gross revenue from the sale of personal data and process or control personal data of at least 25,000 consumers.

Responsibility According to Role

Controllers are responsible for meeting the obligations set forth in the bill. Processors must adhere to instructions of the controller and assist controllers in meeting set obligations. Processing by a processor is governed by a contract between the controller and the processor.

Consumer Rights Requests

A consumer may request to exercise certain rights with regard to their personal data maintained in identifiable form by a controller.

Upon a verified request from a consumer, a controller must:
- confirm if the consumer's personal data is being processed and provide access to such data;
- inform the consumer about third-party recipients or categories with whom the controller shares personal data;
- provide the consumer any personal data that the consumer has provided to the controller in a structured, commonly used, and machine-readable format, if certain conditions are met, such as if the processing is carried out by automated means;
- correct inaccurate personal data of the consumer;
- delete the consumer's personal data, if certain grounds apply, such as when the personal data is no longer necessary for a business purpose; or
- restrict processing, if certain grounds apply, such as when the personal data is being processed is inconsistent with the purpose disclosed to the consumer at the time of data collection.

A controller must communicate any correction, deletion, or restriction of processing carried out pursuant to a consumer's verified request to each third-party recipient to whom the controller knows the personal data has been disclosed, including through a sale, within one year preceding the verified request, unless this proves functionally impractical, technically infeasible, or involves disproportionate effort, or the controller knows or is informed by the third party that the third party is not continuing to use the personal data.

If a consumer objects to processing of their personal data and the processing is for purposes of targeted advertising, the controller must no longer process the personal data subject to objection and communicate the consumer's objection to any known third parties to whom the controller sold the data. If the consumer objects to processing for any purpose other than targeted advertising, the controller may continue processing the personal data if the controller can demonstrate a compelling business purpose to process such personal data.

Controllers may request additional information needed to confirm the identity of the consumer making a request to exercise a consumer right and may charge a reasonable fee to fulfill certain requests.

A controller must respond to received requests within 30 days, unless certain circumstances permit an extension of up to 60 additional days. Controllers must inform consumers within 30 days of any action taken on a request, any extension, and the reasons for the delay or for not taking action.

Transparency

Controllers must be transparent and accountable for their processing of personal data by making available a clear privacy notice that includes certain information, such as the categories of personal data collected and the purposes for which the categories of personal data are used and disclosed to third parties.

Controllers that sell personal data to data brokers or process personal data for targeted advertising must disclose such processing and clearly state the manner in which a consumer may exercise the right to object to such processing.

Risk Assessments

Controllers must conduct and document risk assessments prior to processing personal data when a change in processing materially impacts the risk to individuals and on at least an annual basis.

Risk assessments must take into account the type of personal data to be processed and must identify and weigh the benefits of processing against the potential risks to the rights of the consumer associated with the processing. If the risk assessment determines that the potential risks to the rights of the consumer outweigh the interests of the controller, consumer, and the public, the controller may only engage in such processing with the consumer's consent or if another exemption applies.

Processing for a business purpose shall be presumed to be permissible unless it involves the processing of sensitive data and the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

Risk assessments must be made available to the Attorney General upon request and are exempt from public inspection under the Public Records Act.

Deidentified Data

A controller or processor that uses deidentified data must monitor compliance with any contractual obligations to which deidentified data is subject.

Exemptions.

Local and state governments, municipal corporations, employment records, and certain entities and personal data regulated by federal laws are exempt from the provisions of the act.

The obligations imposed on controllers or processors do not restrict a controller's or a processor's ability to comply with federal, state, or local laws; to comply with a civil inquiry or a criminal

investigation; to cooperate with law enforcement agencies; to investigate, exercise, or defend legal claims; or to prevent or detect fraud or other criminal activity.

Controllers and processors are not required to re-identify deidentified data, to retain personal data that would not otherwise be retained, or to comply with a consumer request if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

Facial Recognition Technology.

Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions that produce legal effects concerning consumers. Processors that provide facial recognition services must prohibit, by contract with controllers, the use of facial recognition services to unlawfully discriminate against consumers.

Controllers must obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public by placing a conspicuous notice regarding the use of facial recognition services. Consumers consent to the use of facial recognition services by entering premises that have such notice.

State and local government agencies are prohibited from using facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces unless in support of law enforcement activities and either: (1) a court order permitting the use of facial recognition services for that ongoing surveillance has been obtained; or (2) there is an emergency involving imminent danger or risk of death to a person.

Liability and Enforcement.

A controller or processor is in violation of this chapter if it fails to cure any alleged violation of this act within 30 days after receiving notice of alleged noncompliance. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

Violations of these provisions are enforceable only by the Attorney General under the Consumer Protection Act and subject to a civil penalty of no more than $2,500 for each violation or $7,500 for each intentional violation. All receipts from the imposition of civil penalties must be deposited into the Consumer Privacy Account. Expenditures from the account may only be used to fund the Office of Privacy and Data Protection.

There is no basis for a private right of action under this act.

The Office of Privacy and Data Protection.

The Office of Privacy and Data Protection (OPDP) must conduct an analysis on the public sector use of facial recognition and submit a report of its findings to the Legislature by September 30, 2023.

In consultation with the Attorney General, the OPDP must establish by rule any exceptions to the bill as necessary to comply with state or federal law, clarify definitions, and create exemption eligibility requirements for small businesses and research institutions.

Appropriation: None.

Fiscal Note: Available for Substitute Senate Bill 5376.

Effective Date: The bill takes effect on July 31, 2021.