Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

HB 1854

Brief Description: Protecting consumer data.

Sponsors: Representatives Kloba, Hudgins, Slatter, Tarleton, Smith, Ryu, Valdez, Stanford and Pollet.

Brief Summary of Bill

- Defines obligations for controllers and processors of personal data who are legal entities that meet specified thresholds.
- Exempts state and local government and certain data sets from the obligations set forth in the act.
- Establishes consumer rights with regard to processing of personal information.
- Makes violations 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 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: 2/12/19

Staff: Yelena Baker (786-7301).

Background:

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.

Personal information and privacy interests are protected under various provisions of state law. The Washington 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:

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.

"Personal data" means any information relating to an identified or identifiable natural person and does not include deindentified data.

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects such as health, economic situation, location, and behavior relating to a natural person.

"Data broker" means a business that knowingly collects and sells or licenses the brokered personal information of a consumer with whom the business does not have a direct relationship.

Consumer Rights.

With regard to processing of personal data, a consumer has the following rights:

- to confirm whether or not personal data concerning the consumer is being processed by the controller;
- to obtain a copy of the personal data undergoing processing;
- to have inaccurate personal data corrected;
- to have personal data deleted where certain grounds apply;
- to restrict processing if certain grounds apply;

- to be provided, in certain circumstances, with any of the consumer's own personal data that the consumer provided to the controller;
- to object to processing of personal data concerning the consumer; and
- to not be subject to a decision based solely on profiling which produces legal effects concerning the consumer.

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 100,000 or more consumers; or
- derive over 50 percent of gross revenue from the sale of personal information and process or control personal information of 25,000 or more consumers.

Consumer Rights Requests.
A controller must facilitate consumer requests to exercise specified consumer rights and may request additional information needed to confirm the identity of the consumer making a request to exercise a consumer right. 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 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 engage in profiling must disclose such profiling to the consumer at or before the time personal data is obtained.

Controllers that sell personal data to data brokers or process personal data for direct marketing 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. Risk assessment must be made available to the Attorney General upon request and are exempt from public inspection under the Public Records Act.

Exemptions.

Local and state governments, employment records, and certain 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 right request if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

Enforcement.

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.

Facial Recognition.

Controllers must obtain consent from consumers prior to deploying facial recognition services. 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.

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 has been obtained; or (2) there is an emergency involving imminent danger or risk of death to a person.

The Office of Privacy and Data Protection 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.

Appropriation: None.

Fiscal Note: Requested on February 7, 2019.

Effective Date: The bill takes effect on December 31, 2020.