HOUSE BILL REPORT
2SSB 5376

As Reported by House Committee On:
Innovation, Technology & Economic Development

Title: An act relating to the management and oversight of personal data.

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 History:
Committee Activity:
Innovation, Technology & Economic Development: 3/22/19, 4/3/19 [DPA].

Brief Summary of Second Substitute Bill
(As Amended by Committee)

- Defines obligations for controllers and processors of personal data and responsibilities for third parties.
- Exempts state and local government, municipal corporations, institutions of higher education, and certain data sets subject to various federal and state laws from the obligations of the act.
- Sets forth specific consumer rights with regard to personal data and requires controllers to fulfill consumer requests to exercise these rights.
- Requires controllers or processors using or providing facial recognition services to meet certain requirements.
- Provides that violations of the act are enforceable under the Consumer Protection Act.
- Prohibits the use of facial recognition technology by all state and local government agencies to engage in surveillance in public places except in specified situations.
- Directs the Office of Privacy and Data Protection to conduct several studies on topics related to consumer data privacy and to report its findings to the Legislature.

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.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: Do pass as amended. Signed by 5 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Slatter, Tarleton and Wylie.

Minority Report: Do not pass. Signed by 4 members: Representatives Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Morris and Van Werven.

Staff: Yelena Baker (786-7301).

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 Amended 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. Personal data includes reidentified data and does not include deindentified data.

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.

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.

Third parties are responsible for assisting controllers and processors in meeting their obligations with regard to personal data third parties receive from controllers or processors. Third parties must comply with consumer requests made known to them by a controller.

Consumer Rights.

A consumer retains ownership in the consumer's personal data processed by a controller, a processor, or a third party, and may exercise certain rights with regard to the consumer's personal data by submitting a request to a controller.

Upon receiving a verified consumer request, 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 in a commonly used electronic format a copy of the consumer's personal data that is undergoing processing;
- 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 the consumer's inaccurate personal data;
- delete the consumer's personal data, if certain grounds apply, such as when the personal data is no longer necessary in relation to the purposes for which it was collected or processed;
- take reasonable steps to inform other controllers or processors that the consumer has requested deletion of personal data;
- restrict processing, if certain grounds apply, such as when the personal data being processed is inconsistent with the purpose disclosed to the consumer at the time of data collection; and
- stop processing the consumer's personal data if the consumer objects to processing and take reasonable steps to communicate a consumer's objection to processing to third parties to whom the controller sold the consumer's personal data.

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.

A controller may request additional information needed to confirm the identity of the consumer making a request to exercise a consumer right and may refuse to act on manifestly unfounded or excessive requests.

A controller must respond to received requests within 30 days, unless certain circumstances permit an extension of up to 60 additional days. Within 30 days of receiving a consumer request, a controller must provide the consumer with information about any action taken on a request, any extension, the reasons for the delay or for not taking action, and information about the process for internal review of the controller's decision.

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 must disclose such sales and provide consumer with information as to how consumers may object to such sales.

Compliance and Risk Assessments.

Controllers must develop, implement, and make publicly available an annual plan for complying with the obligations under the bill, and may report metrics on their public website to demonstrate and corroborate their compliance with these obligations.

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 of privacy harm outweigh the interests of the controller, consumer, and the public, the controller may only engage in such processing with the consumer's consent.

Processing for a business purpose shall be presumed to be permissible unless:

- it involves the processing of sensitive data;
- the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards;

- consent was not given; or
- processing is inconsistent with consent given.

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, sells, or shares deidentified data must:
- make a public commitment to not re-identify deidentified data;
- require by contract that third parties do not re-identify deidentified data received from the controller or processor;
- monitor compliance with any contractual obligations to which deidentified data is subject; and
- address any breaches of contractual commitments related to deidentified data.

Exemptions.

Local and state governments, municipal corporations, and institutions of higher education are exempt from the provisions of the act. In addition, the bill does not apply to the following information:
- health care information subject to certain federal and state laws;
- personal data held by a consumer reporting agency, but solely to the extent that such data is used to generate a consumer report and only if the processing of that personal data is in compliance with the federal Fair Credit Reporting Act;
- personal data regulated by the federal Children's Online Privacy Protection Act, the Gramm Leach Bliley Act, and the Driver's Privacy Protection Act of 1994, if collected, processed, and maintained in compliance with those laws;
- personal data regulated by the federal Family Educational Rights and Privacy Act; and
- employment records.

The obligations imposed on controllers or processors do not restrict a controller's or a processor's ability to conduct a number of specified activities, such as: complying with federal, state, or local laws; complying with a civil inquiry or a criminal investigation; establishing or defending legal claims; protecting against malicious or illegal activity; or processing personal data of a consumer where the consumer has consented to such processing.

The Office of Privacy and Data Protection (OPDP) may grant controllers one-year waivers to permit processing that is necessary for reasons of public health, for archiving purposes, to safeguard intellectual property rights, or to protect the vital interests of a consumer or another natural person.

A controller may not sell any personal data that the controller processes under one of the exemptions or pursuant to a waiver issued by the OPDP.

Controllers and processors are not required to re-identify deidentified data, or to retain or link personal data that would not otherwise be retained or linked.

Facial Recognition Technology.

Prior to using facial recognition technology, controllers and processors must verify, through independent testing, that no variation occurs in the accuracy of the technology on the basis of race, skin tone, ethnicity, gender, or age of an individual. Controllers, processors, and providers of facial recognition technology must notify consumers if an automated decision system makes decisions that produce legal effects or affect legal rights of any Washington resident.

Controllers that use facial recognition technology:
- must obtain consent from consumers prior to collecting or processing any facial recognition data; and
- may not use facial recognition for profiling or to make decisions that produce legal effects concerning consumers.

Processors that provide facial recognition services must:
- provide documentation that explains the capabilities and the limitations of the technology; and
- prohibit by contract the use of the services by controllers to unlawfully discriminate against consumers.

State and local government agencies are prohibited from using facial recognition technology to engage in surveillance in public spaces unless in support of law enforcement activities and either: (1) a court-issued warrant targeting an individual and permitting the use of facial recognition services for that specific, individualized surveillance during a specified limited time frame has been obtained; or (2) there is an emergency involving imminent danger or risk of death to a person, in which case facial recognition may be used for the limited duration of the emergency.

Liability and Enforcement.

Violations of these provisions are enforceable under the Consumer Protection Act.

The Office of Privacy and Data Protection.

The OPDP, in consultation with the Attorney General, must clarify definitions as necessary. The OPDP may create rules for granting controllers one-year exemption waivers to continue processing for specified purposes.

Additionally, the OPDP must:
- conduct an analysis on the public and private sector use of facial recognition and submit a report of its findings to the Legislature by September 30, 2020;
- conduct a study on whether certain federal health information laws adequately protect personal health information and prevent it from being bought, sold, or traded on a

commercial basis, and submit a report of its findings to the Legislature by December 31, 2020; and
- convene a work group to study the best practices for ensuring consumers understand their privacy rights prior to agreeing to Terms of Service, Terms of Agreement, and other similar documents, and to submit a report of its findings and recommendations to the Legislature by July 31, 2021.

Amended Bill Compared to Second Substitute Bill:

The amended bill:

1. sets forth the principle that consumers retain ownership interest in their personal data, including personal data that undergoes processing, and enumerates specific consumer rights with regard to processing of personal data;
2. modifies several key definitions, including "business purpose", "deidentified data", and "facial recognition", and creates new definitions, such as "privacy harm";
3. eliminates the thresholds that a legal entity must meet in order for the obligations set forth in the bill to apply to that entity;
4. exempts certain entities and information subject to enumerated federal and state laws from the provisions of the bill;
5. modifies responsibilities of the controllers and processors, and specifies responsibilities of third parties that receive data from controllers or processors;
6. modifies the provisions related to consumer rights by specifying when controllers must comply with consumer requests to exercise rights, when certain exemptions apply, or what controllers may take into consideration when taking action on consumer requests;
7. adds to the list of information that a privacy notice must contain, such as a statement that the controller processes personal data of a consumer only pursuant to the consumer's consent and solely for the purposes disclosed to the consumer under the privacy notice;
8. requires controllers to develop, implement, and make publicly available an annual plan for complying with the obligations under the bill, and authorizes controllers to report compliance metrics on their public websites;
9. modifies the provisions related to risk assessments, such as by including additional circumstances when processing data for business purposes is not presumed permissible;
10. modifies the provisions related to deidentified data, such as by requiring controllers or processors to make a public commitment not to reidentify deidentified data;
11. modifies the exemptions provisions and authorizes the OPDP to grant one-year waivers to permit processing for certain purposes;
12. prohibits controllers from selling any personal data processed pursuant to an exemption or a waiver;
13. sets forth additional requirements and prohibitions for controllers and processors that use or provide facial recognition services, such as by prohibiting the use of facial recognition for profiling or to make decisions that have legal effects;
14. modifies the enforcement provisions by removing prohibition on the private cause of action; and

15. modifies the rule-making authorization for the OPDP and directs the OPDP to conduct several studies on topics related to consumer data privacy and to report its findings to the Legislature.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on April 4, 2019.

Effective Date of Amended Bill: The bill takes effect July 30, 2020, except for section 15, which takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) The underlying Senate bill presents a thoughtful and deliberate approach by establishing consumer rights and placing affirmative obligations on companies to be responsible stewards of personal data. The exemptions listed in the underlying Senate bill recognize that this bill will be implemented on top of the already-existing legal framework; the bill is also flexible enough to recognize that sometimes there are compelling reasons to continue retaining data.

The underlying Senate bill strikes the right balance for allowing the use of facial recognition technology with proper guidelines; the striking amendment, by contrast, sets up an impossible standard by requiring consent beyond public notice.

The underlying Senate bill is a good compromise document. The private cause of action provided for in the striking amendment is of concern.

(Opposed) Neither the underlying Senate bill nor the striking amendment present a meaningful step forward in terms of privacy protections. As evidenced by academic papers and recent court decisions, there is an expectation of privacy in a public place. There should be a complete moratorium on the use of facial recognition technology which poses unique civil rights concerns. The bias problems with facial recognition are well-known. This technology provides unprecedented surveillance capabilities, and this bill continues to lay the groundwork for a government surveillance infrastructure that produces biased outcomes and unfairly targets vulnerable communities. Setting a low standard with this bill will set a low standard for the whole country.

This bill is weaker than both the European Union's General Data Protection Regulation and California's Consumer Privacy Act and would set a bad precedent. The bill serves the interests of powerful data collectors rather than consumers.

The facial recognition provisions create an expectation of privacy in a public space, which has an implication on the "plain view" doctrine. Consumers would be best served by a federal law that applies across industry sectors rather than a patchwork of state laws. The Attorney General should have the sole authority to enforce the state privacy law.

Requiring health care information to be in compliance with the applicable federal and state laws in order to be exempt sets an impossible standard. Compliance is a process and not as black and white as some would like it to be; health information may be out of compliance without the covered entities being aware of it. The conditional language in the striking amendment does not recognize the existing regulatory structure for medical entities and health care information.

(Other) The striking amendment improves the enforcement mechanisms by adding a private cause of action. Controllers should not use facial recognition to make decisions that produce legal effects, even if a human review is involved. The definition of "sensitive data" should include information about a person's citizenship or immigration status.

The striking amendment removes jurisdictional thresholds, which may create an administrative burden on small businesses. There should be a temporal limitation on the personal data a business processes before that business is subject to the obligations of this bill. Alternatively, there needs to be a limited exemption for land titles and insurance companies. Publicly available data should be excluded from the provision of the bill. "Safe harbor" language should be added in so that a reasonable mistake does not lead to strict liability.

Agencies that use facial recognition software in public safety efforts may suffer setbacks because seeking a warrant every time would be impractical.

The underlying Senate bill provides clarity for consumers and clear directions for businesses, and sets forth a reasonable enforcement mechanism. The tiered private right of action in the striking amendment is of concern. Providing for a private cause of action will not improve compliance but will have a chilling effect on the industries' relationship with regulators.

Persons Testifying: (In support) Senator Carlyle, prime sponsor; Michael Parham, RealNetworks; Ryan Harkins, Microsoft; Julia Gorton, Washington Hospitality Association; Alex Alben, Washington State Office of Privacy and Data Protection; and Mike Hoover, TechNet.

(Opposed) James McMahon, Washington Association of Sheriffs and Police Chiefs; Mark Johnson, Washington Retail; John Christiansen, Christiansen Information Technology Law; Zosia Stanley, Washington State Hospital Association; Shankar Narayan, American Civil Liberties Union of Washington; Samroz Jakvani, Muslim Association of Puget Sound; Eli Goss, OneAmerica; Elise Orlick, WashPIRG; Maureen Mahoney, Consumer Reports; Jevan Hutson, University of Washington Law; Geoff Froh, Densho; Anna Lauren Hoffmann, University of Washington Information School; and Russell Brown, Washington Association of Prosecuting Attorneys.

(Other) Trent House, Washington Bankers Association and United Financial Lobby; Stuart Halsan and Sean Holland, Washington Land Title Association; Michael Transue, Axon; Rose Feliciano, Internet Association; Brad Tower, Toy Association; Bob Battles, Association of Washington Business; Diana Carlen, Relx, Inc; and Emilia Jones, Attorney General's Office.

Persons Signed In To Testify But Not Testifying: None.