SENATE BILL REPORT
SB 5376

As Reported by Senate Committee On:
Environment, Energy & Technology, February 14, 2019

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

Brief Description: Protecting consumer data.

Sponsors: Senators Carlyle, Palumbo, Wellman, Mullet, Pedersen, Billig, Hunt, Liias, Rolfes, Saldaña, Hasegawa and Keiser.

Brief History:
Committee Activity: Environment, Energy & Technology: 1/22/19, 2/14/19 [DPS-WM].

Brief Summary of First Substitute Bill

- Provides that this act will be known as the Washington Privacy Act.
- Identifies controller and processor obligations.
- Requires controllers to facilitate requests to exercise consumer rights regarding access, correction, deletion, restriction of processing, data portability, and objection of direct marketing purposes.
- Requires controllers to conduct risk assessments under certain conditions.
- Specifies the thresholds a business must satisfy for the requirements set forth in this act to apply.
- Provides that this act does not apply to local and state governments, municipal corporations, data regulated by certain federal laws, or employment records.
- Provides that violation of this act violates the Consumer Protection Act.
- 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 of specified individuals in public spaces unless in support of law enforcement or in an emergency.
- Requires the Office of Privacy and Data Protection to conduct an analysis on the public sector use of facial recognition technology.

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.

Majority Report: That Substitute Senate Bill No. 5376 be substituted therefor, and the substitute bill do pass and be referred to Committee on Ways & Means.

Signed by Senators Carlyle, Chair; Palumbo, Vice Chair; Ericksen, Ranking Member; Fortunato, Assistant Ranking Member, Environment; Sheldon, Assistant Ranking Member, Energy & Technology; Billig, Brown, Das, Hobbs, Liias, McCoy, Nguyen, Rivers, Short and Wellman.

Staff: Angela Kleis (786-7469)

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 (PRA) protects a person's right to privacy under certain circumstances if disclosure of personal information: (1) would be highly offensive to the reasonable person, and (2) is not of legitimate concern to the public.

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

The Consolidated Technology Services (CTS) agency supports state agencies as a centralized provider and procurer of certain information technology services. Within the CTS, the Office of the Chief Information Officer (OCIO) has certain primary duties related to information technology for state government, which include establishing statewide enterprise architecture and standards for consistent and efficient operation. Within the OCIO, the Office of Privacy and Data Protection (OPDP) serves as a central point of contact for state agencies on policy matters involving data privacy and data protection.

Summary of Bill (First Substitute): Short Title. This act shall be known as the Washington Privacy Act.

Jurisdictional Scope. This act applies to legal entities that conduct business in Washington State and:

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

This act does not apply to local and state governments; municipal corporations; personal data sets regulated by certain federal laws; or employment records.

Responsibility According to Role. Controllers are responsible for meeting set obligations. 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. Controllers shall facilitate verified requests to exercise consumer rights of access, correction, deletion, restriction of processing, data portability, and objection of direct marketing purposes. The personal data subject to a verified request must be maintained in an identifiable form by the controller. The requirement to facilitate a request does not apply under certain conditions.

Upon verified request from a consumer, a controller must:

- confirm if a consumer's personal data is being processed and provide access to such personal data;
- correct inaccurate consumer personal data;
- delete the consumer's personal data if certain grounds apply such as the data is no longer necessary in relation to the purposes for which the personal data was collected;
- restrict processing if certain grounds apply, such as the accuracy of the personal data is contested by the consumer; or
- provide the consumer any of the their personal data that they provided to the controller.

A consumer may object to the processing of their personal data related to direct marketing, which includes the sale of a consumer's personal data to third parties for direct marketing purposes and targeted advertising. When a consumer objects to direct marketing, 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 direct marketing, the controller may continue processing the personal data if the controller can demonstrate a compelling business purpose to process such personal data.

A controller must respond to a request within 30 days of receipt of the request. Under certain circumstances, this time period may be extended by 60 additional days where reasonably necessary. A controller must notify a consumer within 30 days of receipt of the request (1) if an extension was approved and the reason for the delay; or (2) if no action was taken on a request and the reason for not taking action.

A controller may request additional information to confirm the identity of a consumer if the controller has doubts concerning the identity of the consumer making a request to exercise a consumer right.

Transparency. Controllers must be transparent and accountable for processing personal data by making a privacy notice available that includes certain criteria such as categories of personal data collected and purposes for which the categories of personal data is used and disclosed to third parties. If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, it must disclose such processing, as well as how a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.

Risk Assessments. Controllers must conduct a risk assessments of each of their processing activities involving personal data and any time there is a change in processing that materially increases the risk to consumers. Risk assessments must identify and weigh the benefits of the processing against the potential risks to the rights of the consumer associated with the

processing. If the risk assessment determines the potential risks to the rights of the consumer outweigh the benefits of the processing, the controller may only engage in the processing with the consent of the consumer. Consent shall be as easy to withdraw as to give.

Deidentified Data. A controller or processor that uses deidentified data must monitor compliance with any contractual obligations.

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

Enforcement. A violation of this act violates the CPA. A controller or processor is subject to an injunction and liable for a civil penalty of not 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 OPDP.

Facial Recognition. Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects. In addition, a controller must obtain consumer consent prior to deploying facial recognition services in physical premises open to the public.

All state and local government agencies shall not use facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces unless in support of law enforcement and either: (1) a court order has been obtained; or (2) where there is an emergency.

The Office of Privacy and Data Protection Analysis. 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 31, 2023. In addition, the OPDP, in consultation with the Office of the Attorney General, must establish by rule any exceptions to this chapter necessary to comply with state or federal laws, clarify definitions, and create eligibility requirements for small businesses and research institutions.

EFFECT OF CHANGES MADE BY ENVIRONMENT, ENERGY & TECHNOLOGY COMMITTEE (First Substitute):

- Provides and clarifies definitions.
- Adds exemptions for municipal corporations and for information regulated by state and federal laws.
- Clarifies that controllers shall facilitate requests to exercise consumer rights after the request is verified and that the personal data subject to a verified request is maintained in an identifiable form by the controller.
- Provides conditions under which the right to deletion does not apply.
- Clarifies the conditions under which a controller must restrict processing of a consumer's personal data.
- Removes section regarding a consumer's right to not be subject to a decision based solely on profiling.
- Provides that a controller must communicate any correction, deletion, or restriction of processing to each known third-party within one year preceding the verified request.

- Requires controllers to conduct risk assessments of their processing activities involving personal data and anytime there is a change in processing that materially increases the risk to consumers.
- Removes the requirement for risk assessments to be completed annually.
- Requires controllers to obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public.
- Removes the requirement for notice of the use of facial recognition services to be available online.
- Requires the state privacy office, in consultation with the Attorney General, to establish by rule any exceptions to this chapter necessary to comply with state or federal laws, clarify definitions, and create eligibility requirements for small businesses and research institutions.
- Changes the effective date to July 31, 2021.
- Make technical changes throughout.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: The bill takes effect on July 30, 2021.

Staff Summary of Public Testimony on Original Bill: *The committee recommended a different version of the bill than what was heard.* PRO: Consumers need to have the ability to control their own information. This is a critical moment on the issue of privacy. American companies have had to become compliant with international standards. Those protections should be extended to United States citizens. This bill represents a thoughtful approach taking components from current European, California, and federal laws. The privacy rights in this bill are the strongest in the country and would help businesses compete in international markets.

CON: The exemptions regarding financial information need to be clarified. The language used in the bill regarding facial recognition technology is vague and inflammatory in the industry. Prohibiting the use of facial recognition technology may have unintended consequences such as effecting how the no-flight list is monitored.

OTHER: We think it would be better for states to wait for federal action with regards to privacy. If states are going to take action, then the actions need to be in alignment to ensure companies are not having to manage different requirements across states. Implementation of this bill would be too difficult for small businesses. The thresholds for identifying which businesses this act applies to are too low. We think an effective date of July 2021 is more appropriate because December is the busiest time of the year for retailers. We suggest adding a private right of action and requiring a report to the Legislature on whether or not this model is working. The definition of data sets need to be clarified with regards to financial and healthcare information. Additional research needs to be done on facial recognition technology.

Persons Testifying: PRO: Senator Reuven Carlyle, Prime Sponsor; Julie Brill, Microsoft; Alex Alben, Office of Privacy.

CON: James McMahan, Washington Association Sheriffs and Police Chiefs; Cliff Webster, Consumer Data Industry Association.

OTHER: Trent House, Washington Bankers Association and United Financial Lobby; Mark Johnson, Washington Retail Association; Eric Gonzalez Alfaro, Legislative Director, American Civil Liberties Union of Washington; Shannon Smith, Attorney General's Office; Michael Schutzler, CEO, WTIA; Robert Battles, AWB; Stuart Halsan, Washington Land Title Association; Tom McBride, CompTIA; Rose Feliciano, Internet Association; Rick Gardner, Relx (LexisNexis); Julia Gorton, Washington Hospitality Association; Candice Bock, Association of Washington Cities; Brad Tower, Community Bankers of Washington.

Persons Signed In To Testify But Not Testifying: No one.