Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

2SSB 6281

Brief Description: Concerning the management and oversight of personal data.

Sponsors: Senate Committee on Ways & Means (originally sponsored by Senators Carlyle, Nguyen, Rivers, Short, Sheldon, Wellman, Lovelett, Das, Van De Wege, Billig, Randall, Pedersen, Dhingra, Hunt, Salomon, Liias, Mullet, Wilson, C., Frockt, Cleveland 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, tribes, and certain data sets subject to regulation by specified federal and state laws.
- Establishes consumer personal data rights of access, correction, deletion, data portability and opt-out of the processing of personal data for specified purposes.
- Identifies controller responsibilities, including transparency, purpose specification, data minimization, security, and nondiscrimination.
- Requires controllers to conduct data protection assessments for certain processing.
- Sets forth requirements related to commercial use of facial recognition services.
- Provides that violations are enforceable only by the Attorney General and subject to civil penalties.
- Preempts local laws and ordinances related to the processing of personal data.

Hearing Date: 2/21/20

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.

A sectorial framework protects personal information and privacy interests under various provisions of state and federal law. The Washington Constitution provides that no person shall be disturbed in their private affairs without authority of law. Different state and federal laws define permitted conduct and specify the requisite level of privacy protections for consumer credit records, financial transactions, medical records, and other personal information.

Summary of Bill:

The Washington Privacy Act establishes consumer personal data rights and identifies responsibilities of controllers and processors of personal data, including requirements related to commercial use of facial recognition services.

Key Definitions and Jurisdictional Scope.

"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 deidentified data or publicly available information.

Controllers and processors are legal entities that conduct business in Washington or produce products or services that are targeted to Washington residents and:

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

This act does not apply to state agencies, local governments, tribes, municipal corporations, data maintained for employment records purposes, and information subject to enumerated federal and state laws. Certain personal data are exempt only to the extent that the collection or processing of that data is in compliance with federal and state laws to which the data are subject and which are specified in the exemptions.

Institutions of higher education and nonprofit corporations are exempt until July 31, 2024.

Consumer Personal Data Rights.

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

- confirm whether a controller is processing the consumer's personal data;
- access personal data being processed by the controller;
- correct inaccurate personal data, taking into account the nature of the personal data and the purposes of processing;
- delete personal data;
- obtain in a portable format the consumer's personal data previously provided to the controller; and

- opt out of the processing for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects or similarly significant effects on the consumer.

Except for the right to opt out, the consumer personal data rights do not apply to pseudonymous data where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

A controller is not required to comply with a consumer personal data right request if the controller is unable to authenticate the request using commercially reasonable efforts. A controller must take reasonable steps to communicate a consumer's request to correct, delete, or opt out to each third party to whom the controller disclosed the consumer's personal data within one year preceding the request, unless this proves functionally impractical or involves disproportionate effort.

A controller must inform the consumer of any action taken on a consumer personal data right request within 45 days of receiving the request. This period may be extended once by 45 additional days where reasonably necessary, provided that the controller informs the consumer of the extension and the reasons for the delay within the first 45-day period. If a controller does not take action on a request, the controller must inform the consumer within 45 days of receiving the request and provide reasons for not taking action, as well as instructions on how to appeal the decision with the controller.

Controllers must establish an internal process by which a consumer may appeal a refusal to take action on the consumer's personal data right requests. Within 30 days of receiving an appeal, the controller must inform the consumer of action taken or not taken in response to the appeal and provide a supporting written explanation. Upon request, the controller must provide the written explanation to the Attorney General. With the consumer's consent, the controller must submit the appeal information to the Attorney General. In addition, controllers must provide consumers with an electronic mail address or other online mechanism through which the consumers may submit the results of an appeal and supporting documentation to the Attorney General.

Information provided to a consumer pursuant to a personal data right request must be provided free of charge, up to twice annually. If requests from a consumer are manifestly unfounded or excessive, the controller may charge a reasonable fee or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive nature of the request.

Responsibilities of Controllers and Processors.

Controllers determine the purposes and means of the processing of personal data. Processors process personal data on behalf of a controller pursuant to a contract that sets out the processing instructions, including the nature, purpose, and duration of the processing. Whether an entity is a processor or a controller with respect to specific processing of personal data is a fact-based determination.

Controllers must:

- provide consumers with a clear and meaningful privacy notice that meets certain requirements;
- limit the collection of personal data to what is reasonably necessary in relation to the purposes for which the data are processed, as disclosed to consumers;
- collect personal data in a manner that is adequate, relevant, and limited to what is reasonably necessary in relation to the purpose for which the data are processed, as disclosed to consumer; and
- implement and maintain reasonable data security practices.

A controller or processor that uses deidentified or pseudonymous data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified or pseudonymous data are subject.

In addition, controllers must conduct a data protection assessment of each of the following processing activities:

- the processing for purposes of targeted advertising;
- the sale of personal data;
- the processing for purposes of profiling, where such profiling presents a specified reasonably foreseeable risk;
- the processing of sensitive data; and
- any processing that presents a heightened risk of harm to consumers.

Data protection assessments must identify and weigh the benefits of processing to a controller, consumer, other stakeholders, and the public against the risks to the rights of the consumer. Data protection assessments conducted for the purpose of compliance with other laws may qualify if they have a similar scope and effect.

The Attorney General may request that a controller disclose any data protection assessment relevant to an investigation conducted by the Attorney General and evaluate the assessment for compliance with the controller responsibilities under this act and other laws, including the Consumer Protection Act. Data protection assessments disclosed to the Attorney General are confidential and exempt from public inspection.

Controllers may not:

- process personal data for purposes that are not reasonably necessary to or compatible with the purposes for which the data are processed, as disclosed to consumers, unless pursuant to consumer consent;
- process personal data in violation of state and federal anti-discrimination laws; or
- process sensitive data without consumer consent.

Additionally, controllers may not discriminate against a consumer for exercising consumer rights, including by charging different prices or rates for goods and services or providing a different quality of goods and services to the consumer. The nondiscrimination provision does not prohibit a controller from offering different prices or rates of service to a consumer who voluntarily participates in a bona fide loyalty or rewards program. Personal data collected as part of a loyalty or rewards program may not be sold to a third-party controller unless specified conditions are met.

Processors are responsible for adhering to the instructions and assisting the controller in meeting its obligations. In addition, processors must implement and maintain reasonable security procedures to protect personal data and ensure confidentiality of processing and may engage subcontractors only after specified requirements are met.

Limitations to the Responsibilities of Controllers and Processors.

Controllers and processors are not required to do the following in order to comply with this act:

- reidentify deidentified data;
- comply with an authenticated consumer request to access, correct, delete, or port personal data if specified conditions are met; or
- maintain data in an identified from.

In addition, the obligations imposed on controllers or processors do not restrict a controller's or processor's ability to take certain actions, including:

- comply with federal, state, or local laws;
- provide a product or service specifically requested by a consumer;
- take immediate steps to protect an interest that is essential for the life of a consumer or another natural person, where the processing cannot be manifestly based on another legal basis;
- protect against or respond to an illegal activity;
- engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, if specified conditions are met;
- collect, use, or retain data to conduct internal research solely to improve or repair products, services, or technology;
- collect, use, or retain data to identify and repair technical errors that impair existing or intended functionality; or
- perform solely internal operations that are reasonably aligned with the expectations of a consumer or are otherwise compatible with processing for purposes of performing a contract to which the consumer is a party.

The controller bears the burden of demonstrating that the processing qualifies for an exemption and complies with specified requirements. Personal data that is processed by a controller pursuant to an exemption may be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the exempt purposes. Personal data processed pursuant to an exemption must not be processed for any other purposes.

Commercial use of Facial Recognition Services.

Processors that provide facial recognition services must make available an Application Programming Interface (API) to enable controllers or third parties to conduct independent testing of facial recognition services for accuracy and unfair performance differences across distinct subpopulations. Making an API available does not require the disclosure of proprietary data or if doing so would increase the risk of cyberattacks. If independent testing identifies material unfair performance differences across distinct subpopulations and these results are disclosed to and validated by the processor, the processor must develop and implement a plan to mitigate the identified performance differences.

Processors that provide facial recognition services must provide documentation that plainly explains the capabilities and limitations of the services and enables their testing. Processors must prohibit by contract the use of facial recognition services by controllers to unlawfully discriminate under federal or state law.

Controllers deploying a facial recognition service in physical premises open to the public must provide a conspicuous and contextually appropriate notice that meets certain requirements and obtain a consumer's consent prior to enrolling the consumer's image in the facial recognition service. Controllers are permitted to enroll a consumer's image for security or safety purposes without the consumer's consent, if specified requirements are met.

Controllers that use a facial recognition service to make decisions that produce legal effects or similarly significant effects on consumers must test the service in operational conditions prior to deployment and ensure that the decisions are subject to meaningful human review.

Controllers must conduct periodic training of all individuals who operate a facial recognition service or process personal data obtained from the use of a facial recognition service.

Controllers may not knowingly disclose personal data obtained from a facial recognition service to law enforcement except when the disclosure is:

- pursuant to consumer consent;
- required by law;
- necessary to prevent or respond to an emergency; or
- to the National Center for Missing and Exploited Children.

Voluntary facial recognition services used to verify an aviation passenger's identity in connection services regulated by certain federal laws are exempt from this act. Airlines are required to disclose and obtain customer consent prior to capturing an image. Airlines are prohibited from retaining any images captured with the exempt facial recognition service for more than 24 hours.

Preemption.

Local governments are preempted from adopting any laws, ordinances, or regulations regarding the processing of personal data by controllers or processors.

Liability and Enforcement.

The Attorney General has exclusive enforcement authority. A violation of this act may not serve as the basis for, or be subject to, a private right of action under this act or any other law. A controller or processor that violates this act is subject to an injunction and liable for a civil penalty of not more than $7,500 per violation.

All receipts from the imposition of civil penalties, except for the recovery of costs and attorneys' fees accrued by the Attorney General in enforcing this act, must be deposited into the Consumer Privacy Account created in the state treasury. Moneys in the account may be used only for purposes of the Office of Privacy and Data Protection.

Reports and Research Initiatives.

By July 1, 2022, the Attorney General must submit to the Governor and the Legislature a report evaluating the liability and enforcement provisions of this act, including any recommendations for changes to those provisions.

The Governor may enter into agreements with the governments of British Columbia, California, and Oregon to share personal data by public bodies for the purpose of joint data-driven initiatives. The agreement must provide reciprocal protections that the respective governments agree appropriately safeguard the data.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date: July 31, 2021.