Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

HB 2742

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

Sponsors: Representatives Kloba, Hudgins, Lekanoff 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 subject to regulation by specified federal and state law.
- Establishes consumer personal data rights of access, correction, deletion, data portability, and opt out of the processing of personal data for specified purposes.
- Requires controllers to conduct data protection assessments if specified circumstances apply.
- 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 or ordinances related to processing of personal data.

Hearing Date: 1/22/20

Staff: Yelena Baker (786-7301).

Background:

The Washington Constitution provides that no person shall be disturbed in his private affairs without authority of law. A sectorial framework protects personal information and privacy interests under various provisions of state and federal law. Different laws define permitted

---

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.

conduct and specify the requisite level of privacy protection for consumer credit records, financial transactions, medical records, and other personal information.

The state 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. A private person injured by a violation of the CPA may bring a civil action. A person or entity found to have violated the CPA is subject to treble damages and attorney's fees.

The Office of Privacy and Data Protection (OPDP) was created in 2016 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:

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 de-identified data or publicly available information.

"Processing" means any operation performed on personal data, whether or not by automated means.

"Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. "Processor" means a natural or legal person who processes personal data on behalf of a controller. Determining whether an entity is a processor or a controller with respect to specific processing of personal data is a fact-based determination.

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

This act does not apply to state and local government, municipal corporations, personal data subject to enumerated federal and state laws, or data maintained for employment records purposes.

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 and access the personal data being processed by the controller;
- correct inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing;
- delete the consumer's personal data;
- obtain the consumer's personal data previously provided to the controller in a portable format; and
- opt out of the processing of the consumer's personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decision 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 in cases where the controller is able to demonstrate that it is not in a position to identify the consumer. Additionally, 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.

Within 45 days of receiving a consumer personal data right request, a controller must inform the consumer of any action taken on 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.

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.

Controllers must establish an internal process by which a consumer may appeal a refusal to take action on consumer personal data right requests. If a controller does not take action on the request, the controller must inform the consumer within 30 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. 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. Controllers must also provide consumers with an electronic mail address or other online mechanism through which the consumer may submit the results of the appeal and supporting documentation to the Attorney General. With the consumer's consent, the controller may also submit the appeal information to the Attorney General, who must make publicly available on its website all appeal information, redacted to deidentify individual consumers, that the Attorney General receives from controllers.

Upon request, 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 personal data within one year preceding the consumer's request, unless this proves functionally impractical or involves disproportionate effort.

Responsibilities of Controllers and Processors.

Processing by a processor is governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing. Processors are responsible for adhering to the instructions of the controller and assisting the controller in meeting its obligations. Processors must also implement and maintain reasonable security procedures to protect personal data, ensure confidentiality of the processing, and engage subcontractors only after certain requirements are met.

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 for the specified purposes as disclosed to consumers;
- limit the collection of data to what is adequate and relevant to the specified purposes; and
- establish and implement data security practices.

Controllers may not:

- process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes as disclosed to a consumer;
- process personal data in violation of state and federal anti-discrimination laws;
- discriminate against a consumer for exercising consumer personal data rights; or
- process a consumer's sensitive data without obtaining the consumer's consent.

Additionally, controllers must conduct a data protection assessment of each of their processing activities involving personal data and an additional data protection assessment any time there is a change in processing that materially increases the risk 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. If the assessment determines that the potential risk of privacy harm to the consumer outweigh the interests of the controller, other stakeholders, and the public, the controller may engage in the processing only with the consent of the consumer.

The Attorney General may request, in writing, 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.

Limitations to the Responsibilities of Controllers and Processors.

Controllers or processors are not required to take certain actions in order to comply with this act, such as reidentifying deidentified data or maintaining data in an identified form. A controller or processor that uses deidentified data or pseudonymous data must monitor compliance with any contractual commitments to which pseudonymous or deidentified data are subject.

In addition, several exemptions to the obligations imposed on controllers or processors are specified, including:

- complying with federal, state, or local laws;
- providing a service specifically requested by a consumer;
- conducting internal research;
- processing personal data for public interest; or
- performing internal operations that are reasonably aligned with the expectations of the consumer.

Personal data that is processed by a controller pursuant to an exemption must not be processed for any other purpose than as expressly provided. Personal data processed pursuant to an exemption may be processed solely to the extent that such processing is proportionate and limited to what is necessary in relation to a specified purpose. If a controller processes personal data pursuant to an exemption, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with specified requirements.

Commercial Use of Facial Recognition Services.

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

Processors that provide facial recognition services must make available an application programming interface to enable controllers or third parties to conduct independent testing of facial recognition services for accuracy and unfair performance differences across distinct subpopulations. If independent testing identifies material unfair performance differences across subpopulations and those results are disclosed to the processor and validated, the processor must develop and implement a plan to address the identified performance differences.

Prior to deploying a facial recognition service, controllers must test the facial recognition service in operational conditions and take commercially reasonable steps to ensure best quality results. Controllers must conduct specified periodic training of all individuals that operate a facial recognition service or process personal data obtained from the use of a facial recognition service.

Controllers deploying a facial recognition service in physical premises open to the public must provide a conspicuous and contextually appropriate notice that meets certain minimum requirements and obtain consumer consent prior to enrolling a consumer's image in the facial recognition service, unless four specified requirements are met to permit enrollment without consumer consent.

Controllers that use facial recognition services to make decisions that produce legal effects or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.

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

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

Controllers and processors using a facial recognition service must fulfill controller responsibilities and respond to consumer requests to exercise personal data rights.

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 (Account) created in the state treasury. Moneys in the Account may be used only for purposes of the Office of Privacy and Data Protection (OPDP).

Reports and Research Initiatives.

The OPDP must conduct a study on the development of technology that indicates a consumer's affirmative and unambiguous choice to opt out of the processing of personal data for specified purposes. The OPDP must submit a report of its findings and recommendations to the Governor and the Legislature by October 31, 2021.

The Attorney General must compile a report evaluating the liability and enforcement provisions, including any recommendations for changes to those provisions, and submit a report to the Governor and the Legislature by July 2, 2022.

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

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect on July 31, 2021, except for section 15, relating to the Office of Privacy and Data Protection study, which takes effect 90 days after adjournment of the session in which the bill is passed.