# HOUSE BILL REPORT
# 2SSB 6281

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

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

**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 History:**
**Committee Activity:**
Innovation, Technology & Economic Development: 2/21/20, 2/28/20 [DPA].

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

- 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 under the Consumer Protection Act.

## HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

*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**: Do pass as amended. Signed by 6 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Entenman, Slatter, Tarleton and Wylie.

**Minority Report**: Do not pass. Signed by 3 members: Representatives Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Van Werven.

**Staff**: Yelena Baker (786-7301).

**Background**:

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.

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 Amended 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, including buying and selling 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 meet the following thresholds:

- 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 25 percent of gross revenue from the sale of personal data.

For purposes of these thresholds, "consumer" does not include payment-only transactions where no data about consumers are retained.

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.

The parent or legal guardian of a known child may exercise consumer personal data rights on the child's behalf. If a controller processes personal data of a consumer subject to guardianship, conservatorship, or other protective arrangement, the controller must allow a guardian or conservator to exercise consumer personal data rights on behalf of 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 only as reasonably necessary to provide services requested by a consumer, to conduct an activity that a consumer has requested, or to verify consumer personal data rights requests; 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 processing 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.

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 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. Minimum training requirements are specified, including coverage of meaningful human review, the capabilities and limitations of the service, and its rates of error based on demographical differences among different subpopulations**.**

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 a court-ordered warrant;
- 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 with 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. Local laws, ordinances, or regulations adopted prior to the effective date of the bill are not superseded or preempted**.**

Local laws, ordinances, or regulations regarding facial recognition are not preempted**.**

Liability and Enforcement.

Violations are enforceable under the Consumer Protection Act. 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 December 1, 2020, the Office of Privacy and Data Protection (OPDP) must prepare and post to its public website a report that summarizes the data protected and not protected by this bill, including a list of the types of publicly available information and other information

exempt from the bill. The OPDP may consult with stakeholders in the industry, academia, and consumer and privacy advocacy organizations regarding the scope and coverage of the bill, as well as the appropriate breadth and number of circumstances that limit the obligations of controllers and processors**.**

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.

**Amended Bill Compared to Second Substitute Bill**:

Regarding key definitions and jurisdictional scope, the amended bill:

- specifies in the definition of "consumer" that acting in an individual or household context includes buying and selling in an individual or household context;
- modifies the jurisdictional scope thresholds to make the requirements of the bill applicable to legal entities that control or process personal data of at least 25,000 consumers and derive over 25, rather than 50, percent of gross revenue from the sale of personal data; and
- specifies that certain transactions do not count as "consumers" for purposes of the thresholds that a legal entity must meet before it is subject to the requirements in the bill.

Regarding consumer personal data rights and responsibilities of controllers, the amended bill:

- provides that controllers must allow guardians or conservators to exercise consumer personal data rights on behalf of consumers subject to guardianship or conservatorship; and
- modifies the data minimization responsibility of a controller by requiring that the controller's collection of personal data be only as reasonably necessary to provide services requested by a consumer, to conduct an activity that a consumer has requested, or to verify consumer requests, rather than adequate, relevant, and limited to what is necessary for processing purposes disclosed to consumer.

Regarding the use of facial recognition services, the amended bill:

- removes provisions that permit controllers to enroll a consumer's image in a facial recognition service without first obtaining the consumer's consent;
- requires facial recognition training to include coverage of facial recognition error rates based on demographical differences; and
- permits disclosure of personal data obtained from a facial recognition service to law enforcement when required in response to a court-ordered warrant, rather than a court order, or subpoena or summons issued by a judicial officer or grand jury.

Regarding preemption and enforcement, the amended bill:

- removes provisions related to the private right of action and liability allocation;

- removes provisions giving the Attorney General exclusive enforcement authority and provides that violations are enforceable under the Consumer Protection Act;
- specifies that local laws, ordinances, or regulations regarding the processing of personal data by controllers or processors that are adopted prior to the effective date of the bill are not superseded or preempted; and
- specifies that local laws, ordinances, or regulations regarding facial recognition are not preempted.

Regarding reports, the amended bill:
- requires the Office of Privacy and Data Protection to produce a public report regarding the data protected by the bill.

---

**Appropriation**: None.

**Fiscal Note**: Available.

**Effective Date of Amended Bill**: The bill takes effect on July 31, 2021.

**Staff Summary of Public Testimony**:

(In support) The bill has many meaningful improvements over the last year's version, including the expanded right to delete, the strengthened definition of "deidentified data," and the elimination of broad exemption for business purposes. The bill represents a big step forward in giving consumers data rights that currently do not exist in law, although some companies may already voluntarily provide these rights. This bill is currently the best model for a privacy bill in the country.

The technology sector employs over 300,000 people in Washington; 15,000 technology companies have fewer than 20 employees and have more in common with small retail shops and restaurants than they do with the "Big Tech" companies. The bill carefully balances the privacy interests of consumers and the regulatory burdens on small and large companies.

The bill promotes clarity and interoperability with the existing healthcare information privacy laws that already establish significant privacy protections and heavy oversight at both state and federal level. The exemptions are lengthy because they reflect carefully crafted exemptions for certain information rather than broad entity-based exemptions. It is important to retain the temporal limit on jurisdictional thresholds and the exemptions for publicly available information and information regulated under the federal Gramm-Leach-Bliley Act.

The retail industry uniquely impacts everyone every day, and most retailers are small businesses with fewer than 50 employees. Retailers are fiercely committed to protecting consumers' privacy and their ability to use technology on which they have come to rely. The bill provides clear standards and allows the industry to remain nimble in order to meet the growing demands of today's more sophisticated consumers.

Exclusive enforcement by the Attorney General is appropriate. Consumers still have the right to bring suit under the Consumer Protection Act (CPA) for conduct which amounts to unfair or deceptive practices. The penalties are set at $7,500 per violation, but there will rarely be just a single violation, and those penalties will quickly add up.

(Opposed) Washingtonians deserve a privacy law that fundamentally challenges the business models built on data extraction and exploitation, and not an unenforceable combination of other laws whose sole function is to serve as a national model for industry. This bill has been referred to as the "gold standard," but it is just window dressing. Exemptions and loopholes fill up multiple pages. Allowing secondary uses of data that goes to data brokers and data aggregators does not give consumers a meaningful way to consent to the different uses of their personal information. The opt-out approach to privacy relies on privacy policies and notices that nobody reads; the opt-in model should be adopted instead.

Violations of data privacy can lead to violations of human rights. The internment of the Japanese Americans in 1942 was in part possible because of the breaches of personal information by governmental and private entities, who allowed their records to be used for identification and location of Japanese Americans. Communities of color are concerned about the way that information technology is used to exploit and violate privacy rights of consumers, whose rights are not adequately protected by this bill. Huge sums of money are being made by exploiting the privacy rights of individuals, which is contributing to the current "Golden Age" of income inequality.

Facial recognition has been likened to plutonium-limited beneficial uses, but otherwise extremely dangerous. This bill legitimizes facial recognition technology that is rife with gender and racial biases without meaningful restrictions, without a moratorium that would allow communities to decide if, and not just how, this technology should be used. From the Japanese internment camps to the over policing of the Muslim community after 9/11, history shows that surveillance technology can be abused. Surveillance technology puts immigrants and their families at risk for hostile federal action.

The facial recognition section should be amended to allow controllers to share biometric information with law enforcement when controllers reasonably believe a crime has occurred or is about to occur.

Even if the many loopholes in the bill were closed, the lack of private right of action in the bill eviscerates any meaningful notion of enforcement. Private rights depend on the ability of private citizens to challenge violations of those rights. It is already difficult enough for private citizens, particularly in marginalized communities, to assert their civil rights. Without a private right of action, there is insufficient incentive for companies to comply because the Attorney General will be able to do just a few enforcement actions a year.

Penalties should be higher than $7,500 per violation; by comparison, the European privacy law carries a potential fine of $21 million. The Legislature has a mandate to protect consumers first and foremost; convenience and profits are secondary to that mandate.

Preempting local regulations means that local government would not be able to step up protections, if needed. The bill should be the floor, not the ceiling, and local communities

should be able to make the decisions that work best for them and their community members. Existing local protections concerning privacy and surveillance should not be preempted.

(Other) Consumers' sensitive data are collected, bought, and sold without their consent and, in many cases, without consumers' knowledge, which leaves consumers vulnerable to security breaches or revelations of damaging information. Consumer organizations support the goals of this bill, but it should be made stronger by reinstating the changes made to the companion bill in this committee, including in the definitions of "sale" and "deidentified data," additional protections for teenagers, and enforcement provisions.

Jurisdictional thresholds should be clarified as to whether they include payment-only transactions that do not retain any consumer data. Nonprofit organizations should be exempt from the bill, as they are from the California Consumer Privacy Act.

Most people prefer their online content to be paid for by advertising. The bill should strike the right balance between protecting privacy and enabling responsible tailored advertising, or else it threatens the advertising-support content-rich digital ecosystem.

Facial recognition has been shown to be biased, so it should be tested for bias before being used. Facial recognition is best addressed in a separate bill. Giving controllers license to enroll a consumer's image into a facial recognition service based on reasonable suspicion would give controllers license to profile based on race.

Nonscientific testing of facial recognition can lead to skewed results. The work of the National Institute of Standards and Technology should be leveraged for testing facial recognition. Safety and security exemptions in the facial recognition section should mirror similar exemptions in other parts of the bill.

Private right of action drives frivolous lawsuits and hurts innovation without adding privacy protections for consumers. Pro se litigants could target the news media with frivolous lawsuits.

The Attorney General cannot guarantee meaningful enforcement without making violations per se violations under the CPA and other revisions to provide the Attorney General with proper investigative authority. The CPA is a well-established body of law and a known quantity, both from the standpoint of consumers and the industry. A private right of action along with enforcement by the Attorney General is the best approach.

**Persons Testifying**: (In support) Senator Carlyle, prime sponsor; Jaclyn Greenberg, Washington State Hospital Association; Fielding Greaves, Advanced Medical Technology Association; Michael Schutzler, Washington Technology Industry Association; Ryan Harkins, Microsoft; Sean Holland, Washington Land Title Association; Renee Sunde, Washington Retail Association; and Robert Battles, Association of Washington Business.

(Opposed) Stan Shikuma, Japanese American Citizens League-Seattle Chapter; Larry Behrendt, Indivisible; Livio De La Cruz, Black Lives Matter Seattle; James McMahan, Washington Association of Sheriffs and Police Chiefs; Derek Lum, InterIm Community

Development Association; Eli Goss, One America; Jon Pincus, Indivisible Plus: Washington State; Deborah Pierce; and Jevan Hutson, University of Washington School of Law.

(Other) Maureen Mahoney, Consumer Reports; Joseph Jerome, Common Sense Media; Andrea Alegrett, Office of the Attorney General; Larry Shannon, Washington State Association for Justice; Trent House, Washington Bankers Association; Carolyn Logue, Washington Food Industry Association; Christopher Oswald, Association of National Advertisers; Dustin Brighton, Network Advertising Initiative; Drake Jamali, Security Industry Associations; Alexa Silver, American Heart Association; and Rowland Thompson, Allied Daily Newspapers of Washington; and Jennifer Lee, American Civil Liberties of Washington.

**Persons Signed In To Testify But Not Testifying**: None.