
Civil Rights & Judiciary Committee

2SSB 5062

Brief Description: Concerning the management, oversight, and use of data.

Sponsors: Senate Committee on Ways & Means (originally sponsored by Senators Carlyle, Nguyen, Billig, Darneille, Das, Dhingra, Holy, Hunt, Lovelett, Mullet, Pedersen, Salomon, Sheldon, Wellman and Wilson, C.).

Brief Summary of Second Substitute Bill

- Establishes consumer personal data rights of access, correction, deletion, data portability and opt-out of the processing of personal data for specified purposes.
- Defines obligations for controllers and processors of personal data who are legal entities that meet specified thresholds.
- Identifies controller responsibilities, including transparency, purpose specification, data minimization, security, and nondiscrimination.
- Exempts state and local government, tribes, air carriers, employment-related data, and certain data sets subject to regulation by specified federal and state laws.
- Provides that violations are enforceable only by the Attorney General under the Consumer Protection Act and subject to civil penalties.
- Preempts local laws and ordinances related to the processing of personal data.
- Regulates the processing of data collected for certain public health emergency and contact tracing purposes.

Hearing Date: 3/17/21

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Staff: Yelena Baker (786-7301).

Background:

Federal Laws Related to Privacy.

A sectorial framework protects personal information and privacy interests under various federal laws. Key federal statutes related to privacy include:

- the Health Insurance Portability and Accountability Act (HIPAA), which protects the privacy and security of medical information;
- the Fair Credit Reporting Act (FCRA), which regulates the consumer reporting industry and provides privacy rights in consumer reports;
- the Gramm-Leach-Bliley Act (GLBA), which regulates the sharing of personally identifiable financial information by financial institutions and their affiliates; and
- the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records.

Comprehensive Privacy Laws in Other States.

While no single general privacy law exists at the federal level, two states have recently enacted comprehensive data privacy laws that regulate the collection and sharing of personal information.

The California Consumer Privacy Act (CCPA), which took effect in 2020, regulates the collection, use, and sharing of personal information; and provides California residents with certain data rights, such as the right to access or delete collected personal information and to opt out of the sale of personal information to third parties. In November 2020, California residents approved a ballot initiative titled the California Privacy Rights Act (CPRA), which amends and expands the CCPA and establishes a new enforcement agency dedicated to consumer privacy. The CPRA takes effect January 1, 2023.

Signed into law in early March 2021, the Virginia Consumer Data Protection Act (VCDPA) regulates the collection and use of consumer personal data and grants Virginia residents the rights to access, correct, delete, know, and opt out of the sale and processing of their personal data for targeted advertising purposes. The VCDPA goes into effect January 1, 2023.

Privacy Protection in Washington.

The Washington Constitution provides that no person shall be disturbed in their private affairs without authority of law. Similarly to the federal sectorial approach, different state statutes define permitted conduct and specify the requisite level of privacy protections for medical records, financial transactions, student information, and other personal data.

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. The OPDP also serves as a resource to local governments and the public on data privacy and protection concerns.

Contact Tracing and the Use of Digital Technologies in Public Health.

Case investigation and contact tracing are core public health strategies used to reduce the spread of communicable diseases, such as COVID-19. Case investigation is the identification and investigation of patients with a confirmed and probable diagnosis of a disease. Contact tracing is the subsequent identification, monitoring, and support of a patient's contacts who have been exposed to, and possibly infected with, the virus. In Washington, local health departments, with the support of the Department of Health (DOH), are responsible for performing case investigations and contact tracing.

During the COVID-19 pandemic, digital exposure notification apps and other digital health tools have been developed for use in several countries and states in an effort to reduce reliance on human recall and to facilitate a pandemic response without relying on the resource constraints of traditional contact tracing. In December 2020, the DOH launched an exposure notification technology known as WA Notify, which works by exchanging random anonymous codes with the nearby phones that have WA Notify enabled and anonymously notifies a user if he or she has been in close contact with another user who tested positive for COVID-19. The technology does not know or track users' identity or location, and the exposure notifications do not contain any information about who tested positive or where the exposure may have happened.

Summary of Second Substitute Bill:

Consumer Personal Data Privacy.

Part I of the Washington Privacy Act establishes consumer personal data rights and identifies responsibilities of controllers and processors of personal data.

Key Definitions and Jurisdictional Scope.

"Consumer" means a natural person who is a Washington resident acting only in an individual or household context. "Consumer" 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" 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.

Consumer personal data provisions do not apply to:

- state agencies, legislative agencies, the judicial branch, local governments, municipal corporations, or tribes;
- air carriers;
- data maintained in specified employment-related contexts;
- personal data collected, maintained, disclosed, or otherwise used in connection with the gathering, dissemination, or reporting of news or information to the public by news media; 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, 2026.

Consumer Personal Data Rights.

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

- confirm whether a controller is processing the consumer's personal data;
- access the categories of personal data the controller is processing;
- 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 guardian or conservator may 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. 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. The authentication requirement does not apply to the right to opt out.

A controller must comply with the request to exercise the right to opt out as soon as feasible, but no later than 15 days of receiving the request. A controller must inform the consumer of any action taken on requests to correct, delete, or obtain a copy of the consumer's personal data

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. This period may be extended by 60 additional days, provided that the controller informs the consumer of the extension and the reasons for the delay within the initial 30-day period.

When informing a consumer of any action taken or not taken in response to an appeal, the controller must clearly and prominently provide the consumer with information about how to file a complaint with the Consumer Protection Division of the Office of 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.

A controller must maintain records of all appeals and the controller's responses to appeals for at least 24 months and must compile and provide a copy of appeal records to the Attorney General upon request.

Information provided to a consumer pursuant to a personal data right request must be provided free of charge, up to twice annually. If a request from a consumer is 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 (transparency);
- limit the collection of personal data to what is reasonably necessary, in relation to the purposes for which the data are processed (purpose specification);

- 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 (data minimization); and
- implement and maintain reasonable data security practices (data security).

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:

- processing for purposes of targeted advertising;
- sale of personal data;
- processing for purposes of profiling, where such profiling presents a specified reasonably foreseeable risk;
- 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 complying 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 unless pursuant to consumer consent;
- process personal data on the basis of a consumer's protected characteristic in a manner that unlawfully discriminates against the consumer; 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 requirement 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. If a consumer exercises the right to opt out, 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 controllers in meeting their 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 obtain personal data in a portable format if specified circumstances exist; or
- maintain data in an identifiable form.

In addition, the obligations imposed on controllers or processors do not restrict their 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 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 processed pursuant to an exemption may be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the exempt purposes, and must not be processed for any other purposes.

Enforcement.

A violation of the consumer data privacy provisions may not serve as the basis for a private right of action under this act or any other law. Rights possessed by consumers as of July 1, 2020, under the Consumer Protection Act, the Washington State Constitution, the United States Constitution, or other laws are not altered.

The Attorney General has exclusive enforcement authority under the Consumer Protection Act. Prior to filing a complaint, the Attorney General must provide the controller or processor with a warning letter identifying the alleged violations. If the controller or processor fails to cure any

alleged violation within 30 days, the Attorney General may bring an action against the controller or processor.

A controller or processor that violates this act is subject to an injunction and liable for a civil penalty of up to \$7,500 per violation.

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

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 July 1, 2020, are not superseded or preempted.

Privacy Office Report.

The OPDP, in collaboration with the Attorney General, must research and examine existing analysis on the development of technology, such as a browser or global device setting, indicating a consumer's affirmative choice to opt out of certain processing, and the effectiveness of allowing a consumer to designate a third party to exercise a consumer right on their behalf. The OPDP must submit a report of its findings by December 1, 2022.

Review by the Joint Legislative Audit and Review Committee.

The Joint Legislative Audit and Review Committee (JLARC) must review the efficacy of the Attorney General providing controllers and processors with warning letters and the 30-day period to cure alleged violations. The report must include specified information, such as the number of warning letters sent and a recommendation on whether the Attorney General should continue providing warning letters, or whether the process should be changed or stopped, and if so, when. The JLARC report is due by December 1, 2025.

Data Privacy and Public Health Emergency - Private Sector.

Part II of the Washington Privacy Act establishes consumer rights with regard to covered data processed for covered purposes and identifies responsibilities of controllers and processors.

Key Definitions and Jurisdictional Scope.

"Covered data" includes personal data and one or more of the following: specific geolocation data; proximity data; or personal health data.

"Covered purpose" means processing of covered data concerning a consumer for the purposes of:

- detecting symptoms of an infectious disease;
- enabling the tracking of a consumer's contacts with other consumers, or with specific locations to identify in an automated fashion with whom consumers have come into contact;

- digitally notifying, in an automated manner, a consumer who may have become exposed to an infectious disease; or
- other similar purposes directly related to a state of emergency declared by the Governor and any restrictions imposed under the state of emergency declared by the Governor.

Covered data privacy provisions do not apply to:

- protected health information, as defined in the HIPAA;
- health care information for purposes of state laws governing access to and disclosure of medical records and health care information;
- identifiable private information subject to specified laws and regulations applicable to human subject research;
- information derived from any health care-related information and deidentified in accordance with the HIPAA deidentification requirements;
- information originating from, and intermingled to be indistinguishable with, any exempt health care-related information, if maintained by a health care provider or facility, or other specified entities;
- information used only for public health activities; and
- data maintained for employment records purposes.

Consumer Covered Data Rights.

With regard to processing of covered data for covered purposes, a consumer has the following rights:

- confirm whether a controller is processing the consumer's covered data;
- access the covered data the controller is processing;
- request the correction of inaccurate covered data processed for a covered purpose;
- request the deletion of covered data processed for a covered purpose; and
- opt out of the processing of covered data for a covered purpose.

Consumer covered data rights may be exercised in the same manner as the consumer personal data rights.

Responsibilities of Controllers and Processors.

Controllers that process covered data for a covered purpose have the same responsibilities as controllers that process personal data with regard to privacy notice, purpose specification, data minimization, data security, and anti-discrimination requirements.

It is unlawful for a controller or processor to process covered data for a covered purpose unless the controller or processor provides the consumer with the required privacy notice prior to or at the time of the processing, and the consumer consents to the processing. Additionally, controllers may not:

- process covered data for purposes that are not reasonably necessary to or compatible with the covered purposes unless pursuant to consumer consent;
- process covered data or deidentified data that was processed for a covered purpose for purposes of marketing, developing new products or services, or engaging in commercial

- product or market research;
- disclose any covered data processed for a covered purpose to federal, state, or local law enforcement;
- sell any covered data processed for a covered purpose; or
- share any covered data processed for a covered purpose with another controller, processor, or third party unless pursuant to a contract that meets specified requirements and is disclosed to the consumer in the privacy notice.

A controller must delete or deidentify all covered data processed for a covered purpose when the covered data are no longer being used for the covered purpose.

Limitations to the Responsibilities of Controllers and Processors.

The obligations imposed on controllers or processors of covered data do not restrict their ability to:

- comply with federal, state, or local laws and regulations, or
- process deidentified information to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest if certain conditions are met.

The controller bears the burden of demonstrating that the processing qualifies for an exempt purpose and complies with the requirements applicable to the exempt health care-related information. Covered data processed for exempt purposes may be processed solely to the extent that the processing is necessary, reasonable, and proportionate to these purposes, and must not be processed for any other purposes.

Enforcement.

Violations of the provisions related to covered data are enforced in the same manner as violations of the provisions related to consumer personal data.

Preemption.

Local governments are preempted from adopting any laws, ordinances, or regulations regarding the processing of covered data for a covered purpose by controllers or processors. Local laws, ordinances, or regulations adopted prior to July 1, 2020, are not superseded or preempted.

Data Privacy and Public Health Emergency - Public Sector.

Part III of the Washington Privacy Act identifies the responsibilities of public entities that process technology-assisted contact tracing information.

Key Definitions and Jurisdictional Scope.

"Technology-assisted contact tracing" (TACT) means the use of a digital application or other electronic or digital platform that is capable of independently transmitting information and is offered to individuals for the purpose of notifying, through data collection and analysis, those who may have had contact with an infectious person as a means of controlling the spread of a communicable disease.

"Technology-assisted contact tracing information" (TACT information) means any information, data, or metadata received through technology-assisted contact tracing.

"Controller" means the local government, state agency, or institution of higher education that determines the purpose and means of the processing of TACT information.

"Processor" means a natural or legal person, local government, state agency, or institution of higher education that processes TACT information on behalf of a controller.

Responsibilities of Controllers and Processors.

Responsibilities of controllers and processors that process TACT information are substantively identical to those of controllers and processors that process covered data for covered purposes.

Limitations to the Responsibilities of Controllers and Processors.

Limitations to the responsibilities of controllers and processors that process TACT information are substantively identical to those of controllers and processors that process covered data for covered purposes.

Enforcement.

Any controller that violates, proposes to violate, or has violated the TACT information provisions may be enjoined. Any individual injured by a violation may institute a civil action to recover damages. Where more than one controller or processor, or both a controller and a processor are in violation of this chapter, the liability must be allocated among the parties according to principles of comparative fault.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on March 16, 2021.

Effective Date: The bill contains an emergency clause and takes effect immediately, except sections 1, 2, and 101 through 118, relating to processing of consumer personal data, which take effect July 31, 2022.