HOUSE BILL REPORT
HB 1850

As Reported by House Committee On:
Civil Rights & Judiciary
Appropriations

Title: An act relating to protecting and enforcing the foundational data privacy rights of Washingtonians.

Brief Description: Protecting and enforcing the foundational data privacy rights of Washingtonians.

Sponsors: Representatives Slatter, Berg, Pollet and Harris-Talley.

Brief History:
Committee Activity:
Civil Rights & Judiciary: 1/25/22, 2/2/22 [DPS];
Appropriations: 2/5/22, 2/28/22 [DP2S(w/o sub CRJ)].

Brief Summary of Second Substitute Bill

- Creates the Washington State Consumer Data Privacy Commission vested with administrative powers, and rulemaking and enforcement authority to implement and enforce chapter…, Laws of 2022 (Senate Bill No. 5062).
- Permits a consumer to bring an action for violations of chapter…, Laws of 2022 (Senate Bill No. 5062) after the administrative enforcement process determines that a violation has occurred and if specified requirements are met.
- Imposes an annual fee on controllers and processors of personal data.

HOUSE COMMITTEE ON CIVIL RIGHTS & JUDICIARY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass.

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.

Signed by 9 members: Representatives Hansen, Chair; Simmons, Vice Chair; Davis, Entenman, Kirby, Orwall, Peterson, Thai and Valdez.

Minority Report: Do not pass. Signed by 7 members: Representatives Walsh, Ranking Minority Member; Gilday, Assistant Ranking Minority Member; Graham, Assistant Ranking Minority Member; Abbarno, Klippert, Walen and Ybarra.

Minority Report: Without recommendation. Signed by 1 member: Representative Goodman.

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, which protects the privacy and security of medical information;
- the Fair Credit Reporting Act, which regulates the consumer reporting industry and provides privacy rights in consumer reports;
- the Gramm-Leach-Bliley Act, which regulates the sharing of personally identifiable financial information by financial institutions and their affiliates; and
- the Family Educational Rights and Privacy Act, 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, three states have recently enacted comprehensive data privacy laws that regulate the collection and sharing of personal information.

The California Consumer Privacy Act (CCPA) took effect in 2020 and regulates the collection, use, and sharing of personal information. The CCPA 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, and specifies obligations of businesses that collect and process consumers' personal information.

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, and opt out of the sale and processing of their personal data

for targeted advertising purposes. Under the VCDPA, controllers and processors that collect and use consumers' personal data have obligations of data minimization, purpose limitation, and reasonable data security. The state Attorney General has investigative authority and exclusive authority to enforce violations of the VCDPA. The VCDPA goes into effect January 1, 2023.

Largely following the VCDPA framework, the Colorado Privacy Act grants consumer personal data rights, specifies obligations of controllers and processors that process personal data, and gives the state Attorney General and district attorneys exclusive enforcement authority under the Colorado Consumer Protection Act. The Colorado Privacy Act takes effect July 1, 2023.

Privacy Protection in Washington.
The Washington Constitution provides that no person shall be disturbed in their private affairs without authority of law. As with 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, biometric identifiers, and other personal data.

Washington Consumer Protection Act.
The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General is authorized to investigate and prosecute claims under the CPA on behalf of the state or individuals in the state. A person injured by a violation of the CPA may bring a civil action for injunctive relief, recovery of actual damages, and reasonable attorneys' fees. The courts may increase awarded damages up to three times the actual damages sustained.

Summary of Substitute Bill:

Key Definitions.
"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, household, or consumer device. "Personal data" includes pseudonymous data but does not include deidentified data or publicly available information.

Jurisdictional Scope.
The Washington Foundational Data Privacy Act (FDPA) applies to controllers and processors who 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 sharing of personal data.

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

The FDPA does not apply to:
- state agencies, legislative agencies, the judicial branch, local governments, municipal corporations, or tribes;
- air carriers;
- nonprofit organizations that are registered with the Secretary of State under the Charities Program, collect personal data during legitimate activities related to the organization's tax-exempt purpose, and do not share personal data;
- the National Insurance Crime Bureau, the National Association of Insurance Commissioners, and similar organizations to which any insurer must disclose information related to insurance fraud;
- 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, 2027.

Consent Requirement.
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;
- personal data of a minor for the purposes of targeted advertising or sharing of personal data without obtaining the minor's consent; or
- sensitive data without consumer consent.

Controllers must provide an effective mechanism for a consumer to revoke consent. After a consumer revokes consent, the controller must cease processing the consumer's sensitive data as soon as practicable, but no later than 15 days after revocation.

Consumer Rights Concerning Personal Data.
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 personal data being processed by the controller;
- correct inaccurate personal data;
- 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 sharing 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.

Exercising Consumer Personal Data Rights.
A consumer or a consumer's authorized agent may exercise personal data rights by submitting to a controller a request that specifies which rights the consumer wishes to exercise.

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.

A consumer may exercise the right to opt out of the processing for purposes of targeted advertising or sharing of personal data:
- by designating an authorized agent who may exercise the rights on behalf of the consumer; or
- via user-enabled global privacy controls, such as a browser plug-in or privacy setting or device setting, that communicates the consumer's choice to opt out.

Responding to Consumer Requests to Exercise Personal Data Rights.
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 within 15 days of receiving the request. A controller must inform the consumer of any action taken on requests to access, 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 Washington State Consumer Data Privacy Commission (Commission). 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 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.

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.

Nondiscrimination and Nonretaliation.
Controllers may not process personal data on the basis of a consumer's protected characteristic in a manner that unlawfully discriminates against the consumer.

Controllers may not retaliate 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 nonretaliation 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 shared with a third-party controller unless specified conditions are met.

Data Protection Assessments.
Controllers must conduct a data protection assessment of each of the following processing activities:

- processing for purposes of targeted advertising;
- sharing 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 (CPA). Data protection assessments disclosed to the Attorney General are confidential and exempt from public inspection.

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, or with a civil, criminal, or regulatory inquiry, subpoena, or summons by federal, state, local, or other governmental authorities;
- 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.

To qualify for an exemption, the processing of a consumer's personal data must be reasonably necessary and proportionate for these purposes. 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.

Washington State Consumer Data Privacy Commission.
The Commission is created and vested with full administrative power, authority, and jurisdiction to implement and enforce the FDPA and the rules adopted under the FDPA by the Commission.

The Commission is composed of three members to be appointed by the Governor with advice and consent of the Senate. One of the Commission members must be designated as chairperson by the Governor. The term of each commissioner is five years, with eligibility for reappointment.

The Washington Utilities and Transportation Commission must provide all administrative staff support for the Commission. The Commission may employ staff as necessary to carry out the Commission's duties. The Commission may appoint an executive director to perform the duties as prescribed by the Commission. With certain exceptions, the Commission may delegate to the executive director the powers to implement and enforce the FDPA efficiently and effectively.

Members of the Commission must:

- have qualifications, experience, and skills in the areas of privacy and technology;
- remain free from external influence;
- refrain from any action incompatible with their duties; and
- be precluded, for a period of one year after leaving office, from accepting employment with a controller or processor that was subject to an enforcement action or civil action during the member's tenure or during the five-year period preceding the member's appointment.

The Commission must perform specified functions, including:

- promote public awareness and understanding of risks, safeguards, and rights in relation to the processing of personal data;
- monitor relevant developments related to the protection of personal data;
- provide technical assistance and advice to the Legislature;
- provide guidance, upon request, to controllers and processors regarding their obligations;
- establish a data protection certification mechanism; and
- conduct data protection audits of controllers and processors.

In addition, the Commission must adopt rules to carry out the purposes of the FDPA, including adopting rules to:

- amend and update as needed the definitions to address the changes in technology and privacy concerns;
- facilitate and govern the submission of requests by consumers, with the goal of minimizing the administrative burden on consumers while taking into account available technology and the burden on controllers;
- govern controllers' compliance with consumers' requests and the processing of personal data for exempt purposes; and
- establish any exceptions as necessary to comply with state or federal laws, including those relating to trade secrets and intellectual property rights.

The Commission may adopt additional rules as necessary, with the goal of strengthening consumer privacy and incorporating public input, while considering the legitimate operational interests of controllers and processors.

Annual Registration Requirement.
Controllers and processors must register annually with the Commission and provide certain information regarding their personal data processing operations, including:

- whether the controller or processor offers an opt-in or opt-out model for its personal data processing operations and how a consumer can access these options;
- a statement specifying the methods used for personal data processing operations and databases maintained; and
- a statement specifying the number of Washington consumers about whom personal

data was collected, processed, or shared in the preceding year.

Upon registration, controllers and processors must pay a $250 or $450 registration fee, depending on the controller or processor's annual gross revenue in the year preceding registration.

A controller or processor that fails to register is subject to a fine between $1,000 and $20,000 for each day it fails to register. A controller or processor that knowingly submits false or incomplete information upon registration is subject to a fine between $10,000 and $100,000. All fines must be levied by the Commission. When determining the amount of fines to be levied, the Commission must consider factors such as the controller or processor's gross annual revenue and assets, and whether the controller or processor made reasonable efforts to comply with the registration requirements.

Administrative Enforcement by the Consumer Data Privacy Commission.
Upon the complaint of a consumer or on its own initiative, the Commission may investigate alleged violations by a controller or processor or refer the complaint to the Attorney General. The Commission and the Attorney General may consult prior to referral to determine the appropriate enforcement mechanism. Taking into consideration certain factors, such as the lack of intent to violate, the Commission may decide not to investigate a complaint.

At least 30 days prior to the Commission's consideration of the alleged violation, the Commission must provide the alleged violator with a notice of the alleged violation and a summary of the evidence, and inform the alleged violator of the right to be present in person and presented by counsel at any proceeding by the Commission. A proceeding held for the purpose of considering whether there is reason to believe that a violation has occurred is private unless the alleged violator files with the Commission a written request that the proceeding be public.

If the Commission determines there is reason to believe that a violation occurred, the Commission must issue a warning letter identifying specific provisions the Commission believes have been or are being violated. Within 30 days of the issuance of the warning letter, the controller or processor must provide the Commission with a written response that either explains that the alleged violation has not been committed or summarizes how the violation has been cured. Upon the receipt of the controller or processor's response, the Commission must make a written finding as to whether a violation has occurred and whether it has been cured. The Commission must close the matter if it finds that no violation has been committed or that the violation has been cured.

If the Commission makes a written finding that the violation has not been cured, the Commission may proceed with the administrative hearing to determine if a violation has occurred. Notice must be given and the hearing conducted in accordance with the Administrative Procedure Act.

If the Commission determines that no violation has occurred, it must publish a declaration so stating. If the Commission determines that a violation has occurred, the Commission shall issue an order that may require the violator to:

- cease and desist the violation; or
- pay an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation and each violation involving a minor's personal data.

Any decision of the Commission is subject to judicial review.

Civil Enforcement by the Attorney General.
The Attorney General may enforce the FDPA under the CPA. In actions brought by the Attorney General, a violation of the FDPA is a per se violation of the CPA. No action may be filed by the Attorney General for any violation by a controller or processor after the Commission has issued a decision against that controller or processor for the same violation.

Until July 1, 2024, 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.

Private Right of Action.
A consumer may bring a civil action for the violations of the FDPA under the CPA. The legislative declarations establishing a violation of the FDPA as a per se violation of the CPA do not apply to actions brought by consumers.

Thirty days prior to filing an action, a first-party claimant must provide written notice of the basis for the action to the defendant and the Commission. If the defendant fails to resolve the basis for the action within the 30-day period, the claimant may bring the action without any further notice.

Annual Fee on Data Collectors.
Beginning on or after January 1, 2023, an annual fee is imposed upon every data controller or data processor that is required to register with the Commission. The Commission must share with the Department of Revenue a complete directory of all data controllers and processors registered with the Commission for the purposes of assessing the annual fee.

Consumer Privacy Account.
All receipts from the registration fees, imposition of administrative fines and civil penalties, and the annual data collectors fee must be deposited into the Consumer Privacy Account created in the State Treasury. Moneys in the account may only be used for the Commission and for the recovery of costs and attorneys' fees accrued by the Attorney General.

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, 2021, are not superseded or preempted.

Substitute Bill Compared to Original Bill:

The substitute bill makes the following changes to the original bill:

1. modifies the definition of "share" by no longer exempting from the definition certain types of personal data disclosures or transfers, such as disclosures to processors and affiliates, or transfers of personal data as an asset that is part of a merger or an acquisition;
2. modifies the definition of "targeted advertising" by: providing that "targeted advertising" means obtaining information about a consumer to display an advertisement based on the consumer's personal data, rather than displaying an advertisement based on the consumer's personal data; and no longer excluding from the definition advertising based on activities within a controller's own commonly branded websites or applications;
3. exempts from the bill the National Insurance Crime Bureau, the National Association of Insurance Commissioners, and similar organizations to which any insurer or licensee of the state Insurance Commissioner must disclose information related to insurance fraud;
4. removes the requirement to take into account the nature of the personal data and the purposes of processing from the consumers' right to correct inaccurate personal data;
5. requires controllers and processors, when registering with the Washington State Consumer Data Privacy Commission (Commission), to specify the number of data subjects globally about whom personal data was collected, processed, or shared in the preceding year, instead of specifying the amount of personal data collected, processed, or shared in the preceding year;
6. requires controllers and processors, when registering with the Commission, to specify the number of Washington consumers about whom personal data was collected, processed, or shared in the preceding year, instead of specifying the amount of personal data of Washington consumers collected, processed, or shared in the preceding year;
7. specifies the areas in which the Commission must adopt rules, including amending and updating definitions, establishing rules and procedures to govern the submission of consumer data rights requests and the controllers' compliance, defining the technical specifications for global privacy controls, and establishing any exceptions as necessary to comply with state or federal law, such as those related to trade secrets and intellectual property rights;
8. modifies the administrative enforcement process by requiring the Commission to issue a warning letter, make a written findings based on the response to the warning letter, and close the matter if the Commission finds that the alleged violation has not been committed or has been cured;

9. removes the requirement for the Commission to stay an administrative action upon the Attorney's General request and instead permits the Commission to consult with the Attorney General to determine the appropriate enforcement mechanism prior to referring a complaint to the Attorney General;
10. modifies the private right of action by providing that, instead of a civil action in superior court to enjoin further violations and to recover actual damages, a person may bring a civil action under the Consumer Protection Act;
11. delays the effective date of the bill by one year, to July 31, 2023, with the exception of the intent section, and the three sections that create the Commission, specify its duties, and authorize the Commission to promulgate rules, all of which take effect July 31, 2022; and
12. delays by one year the expiration date for the right to cure in the civil enforcement provisions, to reflect the delayed effective date for the bill.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

Effective Date of Substitute Bill: The bill takes effect on July 31, 2023, except for sections 1, 2, and 14 through 16 relating to the Consumer Data Privacy Commission, which take effect July 31, 2022.

Staff Summary of Public Testimony:

(In support) This bill recognizes privacy as a fundamental right and seeks to provide a foundational privacy regulatory framework to protect individuals' privacy, establish clear and equitable ways for consumers to exercise control over their data, and require companies to be responsible custodians and stewards of consumers' data. Many privacy watchers and members of the technology industry agree that regulations are vital, but for the last three years there has not been agreement on the focus of these policies. This bill is different because it creates a new agency to investigate violations and enforce privacy rights. The agency would provide predictability to the industry and an important pathway for consumers, in parallel with a limited private right of action that contains a right to cure.

This bill is foundational; it is an absolute baseline for privacy rights, and those rights are not a one-time conversation. As technology advances, conversations around privacy will have to continue, and this bill is just the first step. The privacy agency will have authority to keep these privacy requirements up to date as technology progresses.

This bill extends to consumers important privacy rights and takes steps to ensure that consumers can practically exercise their rights, including by requiring companies to honor global opt-out signals. The definitions have been clarified to ensure that the rights are meaningful and to tighten potential loopholes in the language concerning exemptions.

There is a threshold to ensure that small companies are not inappropriately impacted by this bill.

If companies are not going to face real consequences for violations, then any requirements to keep data private and secure are meaningless. It is important for the Attorney General to continue to have a strong role in enforcing this bill. The enforcement model in this bill strikes a good balance, with vibrant roles for consumers to enforce their own rights along with the public enforcement pieces to address violations. The private right of action in this bill does not open the floodgates of litigation because these types of claims remain highly technical and extremely expensive to bring. Compensation for reputational harm should be struck from the definition of "actual damages" in the private right of action provisions.

Any effective privacy bill needs to be based on the opt-in, rather than opt-out, model.

(Opposed) In addition to the private right of action, this bill creates a new commission with enforcement responsibilities but no opportunity for well-meaning businesses to cure any errors. Managing personal data and consumer data rights is operationally very complicated, and accidental mistakes can be very common. Businesses are going to be harassed with civil actions for any alleged highly technical or operational failure to comply with consumer rights, and any unintentional or perceived violation could result in ruinous liability for companies. This bill would enable class action firms to wield the statute as a cudgel against well-meaning businesses in order to extract significant settlements, with little or no actual value delivered to the consumer.

The inclusion of three enforcement mechanisms in the bill is unprecedented and overly broad, and would inevitably lead to numerous nuisance lawsuits without creating meaningful protection for consumers. There should be a requirement to choose only one enforcement mechanism. Private right of action should be removed. Central enforcement by the Attorney General, with a right-to-cure period, ensures that justice is meted out evenly and that enforcement actions are targeted to those causing actual harm to Washingtonians, not just those that offer an opportunity for a lucrative settlement.

There are no age parameters as to who can exercise consumer rights and how long data must be maintained. The bill allows any adult to exercise the rights of access, correction, and deletion for any data collected from them when they were under the age of 18. This is in direct conflict with other provisions of the bill that prohibit companies from maintaining data for longer than necessary to fulfill a transaction or provide a service.

It is estimated that a patchwork of different state privacy laws is going to cost businesses as much as $1 trillion over the next 10 years. The bill creates a registration fee and a separate data collection fee that has not been defined; it effectively appears to be a data tax.

(Other) Lack of strong privacy regulations for the past two decades of rapid technology advancement has created the illusion that people must simply accept the entitlement of

businesses to collect, retain, and sell personal data. This bill does not break with that presumption. Washington has an opportunity to pass the strongest data protection in this country and should reject measures that will entrench a status quo that is in desperate need of change. Elements of other privacy proposals should be incorporated into this bill before this can be considered the minimum standard for a strong privacy bill.

An opt-out framework with a litany of loopholes and exemptions is a status quo that will not meaningfully empower people to control their information. To create meaningful privacy protections, start with a full opt-in model. Opting out for sensitive data does not provide the protections that are needed, is unreasonably complex, and can take weeks and upwards of a $1,000 to address. The problem with the opt-out approach is that having to track down one's own data is a great burden that makes it harder for consumers to protect themselves from unwanted attention, like stalking or online harassment. An opt-in framework would protect families from stalking and scams and make democracy safer.

A privacy bill must protect consumers for real-world data abuses that happen today, such as educational technology companies targeting advertising to students by combining personal information with psychological surveys schools require students to take, or data brokers selling personal data to federal government contractors without consumers' consent. To provide the strongest protections, other privacy proposals, written in conjunction with the communities most harmed by data abuses, should be considered.

The threat of violence online crosses aisles and affects people of all political persuasions. In many cases, people are also targeted by abusive partners or fraudulent scammers, and local law enforcement is often helpless because of the technical sophistication of the violence. These risks exist because of the unmitigated danger of the data brokers industry which frequently partners with big companies like Facebook or Google and retail businesses. As written, the bill would continue to allow companies like Facebook or Google to sell people's data to other companies and data brokers without consent.

The preemption clause should be eliminated. The exemption for data sharing between affiliates should be eliminated. The definition of "affiliate" would allow Facebook to share personal data with Instagram without consumers' knowledge or consent or ability to prevent sharing or opt out. For consistency, the definitions of "personal data" should be revised to mean data linked to a consumer, rather than to a natural person.

The enforcement mechanisms are insufficient. Any legislation that includes the right to cure is anti-consumer and should be rejected. The bill should have a full, instead of a limited, private right of action, with full statutory penalties and attorneys' fees because large data companies should be subject to the same consumer protection as other industries. Any provision related to the new commission that limits the enforcement authority of the Attorney General should be removed. If the bill is made less consumer-friendly, Washingtonians are better off with the existing protections.

A comprehensive national framework would provide consumers meaningful rights over their personal data and require businesses to use that data in line with consumers' expectations.

Persons Testifying: (In support) Representative Vandana Slatter, prime sponsor; Representative April Berg; Maureen Mahoney, Consumer Reports; Alexander Zamora, University of Washington Law Technology Policy Clinic; and Larry Shannon and Ian Birk, Washington State Association for Justice.

(Opposed) Molly Jones, Washington Technology Industry Association; David Edmonson, TechNet; Robert Battles, Association of Washington Business; Maya McKenzie, Entertainment Software Association; and Anton van Seventer, DLA Piper.

(Other) Jonathan Pincus, Indivisible Plus Washington; Tom Foulkes, BSA; Lindsey Stewart, ZoomInfo; Maya Morales; Andrea Allegret, Washington State Attorney General's Office; Praveen Sinha, Equality Labs; Savannah Sly; Stanley Shikuma, Japanese American Citizens League Seattle Chapter; Jennifer Lee, American Civil Liberties Union of Washington; and Rowland Thompson, Allied Daily Newspapers and Washington State Association of Broadcasters.

Persons Signed In To Testify But Not Testifying: None.

HOUSE COMMITTEE ON APPROPRIATIONS

Majority Report: The second substitute bill be substituted therefor and the second substitute bill do pass and do not pass the substitute bill by Committee on Civil Rights & Judiciary. Signed by 17 members: Representatives Ormsby, Chair; Gregerson, Vice Chair; Macri, Vice Chair; Chopp, Cody, Dolan, Fitzgibbon, Frame, Hansen, Johnson, J., Lekanoff, Ryu, Senn, Springer, Stonier, Sullivan and Tharinger.

Minority Report: Do not pass. Signed by 15 members: Representatives Bergquist, Vice Chair; Stokesbary, Ranking Minority Member; Chambers, Assistant Ranking Minority Member; Corry, Assistant Ranking Minority Member; MacEwen, Assistant Ranking Minority Member; Boehnke, Caldier, Chandler, Dye, Harris, Hoff, Jacobsen, Rude, Schmick and Steele.

Minority Report: Without recommendation. Signed by 1 member: Representative Pollet.

Staff: Jessica Van Horne (786-7288).

Summary of Recommendation of Committee On Appropriations Compared to Recommendation of Committee On Civil Rights & Judiciary:

The second substitute bill removes provisions that establish consumer data rights, define obligations for controllers and processors, require annual registration by controllers and

processors, and authorizes the Attorney General to enforce violations under the Consumer Protection Act (CPA).

The second substitute bill modifies provisions related to the Washington State Consumer Data Privacy Commission (Commission) and:

- vests the Commission with the authority to implement and enforce chapter…, Laws of 2022 (Senate Bill No. 5062), which addresses the removed provisions, rather than the original bill;
- staggers the 5-year terms of the commissioners;
- removes the specific subjects on which the Commission is required to promulgate rules and instead provides that the Commission must adopt suitable rules to carry out the purposes of the administrative enforcement and annual fee provisions, as well as chapter…, Laws of 2022 (Senate Bill No. 5062);
- removes the requirements that the Commission: establish data protection mechanisms; conduct data protection audits of controllers and processors; and encourage the formation of codes of conduct by controllers and processors;
- requires the Commission to cooperate with other jurisdictions with similar consumer data privacy laws;
- requires the Commission to conduct an analysis of any global privacy control mechanism for the purposes of opting out of certain processing of personal data;
- requires the Commission to establish and maintain a publicly accessible website with the information provided by controllers pursuant to the annual registration requirement in Second Substitute Senate Bill 5062; and
- permits the Commission to consult with the Office of Privacy and Data Protection.

The second substitute bill modifies provisions related to private right of action and:

- provides that the consumer may bring an action under the CPA only after the Commission determines in an administrative hearing under the Administrative Procedure Act that a violation has occurred, rather than authorizing a consumer's action in parallel with the administrative enforcement process;
- requires the Commission to determine that the consumer suffered actual damages before the consumer may proceed with a CPA action;
- authorizes a consumer to bring a CPA action if the Commission's cease and desist order is not being complied with and the consumer suffers actual damages due to noncompliance; and
- defines "actual damages" as demonstrable economic loss or physical harm to the consumer as a result of the violation.

The second substitute bill modifies provisions related to the annual fee imposed on controllers and processors and:

- replaces an unspecified annual fee with the requirement that every controller and processor that meets the jurisdictional thresholds in chapter…, Laws of 2022 (Senate Bill No. 5062) pay to the Commission a fee equal to 0.1 percent of intrastate gross operating revenue;

- makes the annual fee continent on an interagency agreement between the Commission and the Department of Revenue and subject to state law that regulates the disclosure of tax information and tax returns;
- provides that submitted gross revenue information is confidential and privileged and prohibits the Commission or any other person from disclosing any gross revenue information;
- exempts from the annual fee any controller or processor with the intrastate gross operating revenue below $20 million in the preceding year;
- mandates that the collected fees do not exceed $10 million a year, instead of authorizing the Commission to set by rule that the collected fees do not exceed that limit;
- authorizes the Commission to reduce or increase by rule the percentage of intrastate gross operating revenue that is used to determine the annual fee; and
- specifies that the annual fee receipts must be deposited into the Consumer Privacy Account.

The second substitute bill contains a contingent effective date and provides that the act takes effect only if chapter…, Laws of 2022 (Senate Bill No. 5062) becomes law by July 1, 2022. The second substitute bill also contains a null and void clause, making the bill null and void unless funded in the budget.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Second Substitute Bill: This bill takes effect 90 days after adjournment of the session in which the bill is passed, except for section 3, concerning administrative enforcement, which takes effect July 31, 2023. However, the bill only takes effect if chapter…, Laws of 2022 (2SSB 5062) becomes law by July 1, 2022. Additionally, the bill is null and void unless funded in the budget.

Staff Summary of Public Testimony:

(In support) Personal data fuels the digital economy, and large amounts of data are generated about us online. The rules for collecting and using personal data have not been established in Washington. Ordinary people feel that privacy does not exist anymore because they do not feel empowered or knowledgeable about privacy and technology. Privacy does exist, and there is a better way to set up the rules and make decisions in this very complex area.

This bill is a foundational privacy framework, and it creates a commission that will provide and enforce clear rules of the road to the industry. Ordinary people will have a way to address their privacy concerns even if they do not have the means to hire an attorney. This is the result of several years' worth of hard work and gives consumers strong privacy

protections, including the global opt-out and narrowed exemptions. Strong and thoughtful enforcement provisions of this bill are key to giving consumers an opportunity to hold giant technology companies accountable for violating consumer data rights. Based on research from other states, concerns about frivolous litigation have not borne out over time.

The bill imposes an annual fee on companies that extract or use large amounts of Washingtonians' data. This fee will be limited to $10 million annually and will be used solely for operating the new commission.

(Opposed) The technology industry supports strong privacy protections for Washingtonians, but this bill significantly undermines the framework of a good privacy bill and jeopardizes the functioning of online applications and tools. There are serious concerns about the lack of definitional consistency with other states and undefined fees that appears to be a data tax.

The inclusion of three enforcement mechanisms is unprecedented and overly broad, and would lead to numerous nuisance lawsuits without creating meaningful protections for consumers. Allowing the private right of action means that any unintentional violation could result in ruinous liability for companies. Central enforcement by the Attorney General and the right to cure ensures that justice is meted out evenly, and that enforcement actions are targeted at those causing actual harm to Washingtonians.

Hospitality businesses collect data, such as contact information, to communicate with customers and for brand loyalty programs, which are designed to generate recurring business. Small businesses in every industry and sector are disproportionately affected by this bill.

(Other) The deletion requirement appears to require deletion not only of the data provided by a consumer, but all data about a consumer, including data obtained from third parties. This requirement presents a problem for companies that collect data from third parties. These companies could delete the data when requested, but they constantly get streams of updated new data. If these companies hold back some identifying data so that they can delete the consumers' new incoming data, they would be in violation of the deletion requirement. The deletion requirement should be limited to deleting directly provided data; alternatively, companies should be allowed to treat deletion requests as opt-out requests.

While this is an improvement on past bills, this bill still does not meet the minimum requirements for a strong privacy bill. Not enough resources are allocated to the new privacy commission; countries whose population is a tenth of Washington's spend 10 times more a year to fund their data protection agencies. The right to cure is a costly barrier to meaningful enforcement. Government agencies and nonprofits are exempt from this bill, yet these entities also collect and share data.

Persons Testifying: (In support) Representative Vandana Slatter, prime sponsor; Maureen Mahoney, Consumer Reports; and Larry Shannon, Washington State Association for

Justice.

(Opposed) David Edmonson, TechNet; Molly Jones, Washington Technology Industry Association; Robert Battles, Association of Washington Business; and Julia Gorton, Washington Hospitality Association.

(Other) Philip Recht, Mayer Brown Limited Liability Partnership; Jennifer Lee, American Civil Liberties Union of Washington; and Maya Morales, Washington People's Privacy Network.

Persons Signed In To Testify But Not Testifying: None.