HOUSE BILL REPORT
HB 2742

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: Representatives Kloba, Hudgins, Lekanoff and Pollet.

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 1/22/20, 2/7/20 [DPS].

Brief Summary of Substitute Bill

- Defines obligations for controllers and processors of personal data.
- Exempts state and local government, certain data sets subject to regulation by specified federal and state law, and legal entities that meet certain limits.
- Establishes consumer personal data rights of access, correction, deletion, data portability, and opt-out of the processing of personal data.
- 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.
- Provides that violations are enforceable under the Consumer Protection Act and subject to civil penalties.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 6 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Entenman, Slatter, Tarleton and Wylie.

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.

Minority Report: Do not pass. Signed by 2 members: Representatives Smith, Ranking Minority Member; Van Werven.

Staff: Yelena Baker (786-7301).

Background:

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

The state Consumer Protection Act (CPA) prohibits unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General may investigate and prosecute claims under the CPA on behalf of the state or individuals in the state. A private person injured by a violation of the CPA may bring a civil action. A person or entity found to have violated the CPA is subject to treble damages and attorney's fees.

Summary of Substitute Bill:

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

Key Definitions and Jurisdictional Scope.

"Consumer" means a natural person who is a Washington resident acting only in an individual or household context and does not include a natural person acting in an 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.

"Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. "Processor" means a natural or legal person who processes personal data on behalf of a controller. Controllers and processors are legal entities that conduct business in Washington or produce products or services that are targeted to Washington residents.

This act does not apply to:

- state and local government;
- municipal corporations; or
- legal entities that have fewer than 10 employees and less than $5 million in gross annual revenues, derive less than 5 percent of annual gross revenues from the sale or

monetization of personal data, and meet other specified limits with regard to processing of personal data.

In addition, personal data subject to enumerated federal and state laws are exempt from the provisions of this act. Certain personal data are exempt only to the extent that the collection or processing of that data is in substantial compliance with federal and state laws to which the data are subject and which are specified in the exemptions. Data maintained for employment records purposes are exempt until July 31, 2022.

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;
- delete personal data;
- obtain in a portable format the consumer's personal data previously provided to the controller; and
- opt out of the processing of personal data.

If a controller processes personal data of a known child, the controller must allow a parent or legal guardian of the child to 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.

A controller must take reasonable steps to communicate a consumer's request to correct, delete, or opt out to each third party to whom the controller disclosed the personal data within one year preceding the consumer's request, unless this proves functionally impractical or involves disproportionate effort.

Except for the right to opt out, the consumer personal data rights do not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical, contractual, and organizational controls that prevent the controller from accessing such information. Additionally, a controller is not required to comply with a consumer right request if the controller is unable to authenticate the request.

Within 21 days of receiving a consumer personal data right request, a controller must inform the consumer of any action taken on the request. This period may be extended once by 45 days where necessary, provided that the controller informs the consumer of the extension and the reasons for the delay within the initial 21-day period. Controllers must establish an internal process by which a consumer may appeal a refusal to take action on consumer personal data right requests.

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 must:

- provide consumers with a clear and meaningful privacy notice that meets certain requirements;
- limit the collection of personal data to what is necessary in relation to the purposes for which personal data are processed, as disclosed to consumers;
- limit the collection of data to only what is reasonably necessary to provide services or conduct an activity requested by a consumer, or to verify consumer rights requests; and
- establish and implement data security practices.

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 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 necessary to or compatible with the purposes for which personal data are processed, as disclosed to consumers;
- process personal data in violation of state and federal antidiscrimination laws; or
- process a consumer's sensitive data without obtaining the consumer's 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 reward program. Personal data collected as part of a loyalty program may not be sold to a third-party controller unless certain specified conditions are met.

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

Limitations to the Responsibilities of Controllers and Processors.

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

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

- complying with federal, state, or local laws;
- providing a service specifically requested by a consumer;
- protecting vital interests of a consumer or another natural person;
- processing personal data to conduct ongoing scientific, historical, or statistical research in the public interest, if certain specified conditions are met;
- conducting internal research to improve or develop products, services, or technology; or
- performing internal operations that are aligned with the expectations of the consumer.

The controller bears the burden of demonstrating that the processing qualifies for the 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 such processing is necessary and proportionate to what is necessary in relation to a specified purpose. Personal data processed pursuant to an exemption must not be processed for any other purpose.

Commercial Use of Facial Recognition Services.

Prior to deploying a facial recognition service, processors that provide facial recognition services must make available an application programming interface to enable controllers or third parties to conduct independent testing of facial recognition services for accuracy and unfair performance differences across distinct subpopulations. If independent testing identifies material unfair performance differences across subpopulations and those results are disclosed to the processor and validated, the processor must develop and implement a plan to 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 testing of the services. Processors must prohibit by contract the use of facial recognition services by controllers to unlawfully discriminate under federal or state law.

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

Controllers deploying a facial recognition service in physical premises open to the public must provide a conspicuous and contextually appropriate notice that meets certain minimum requirements and obtain consumer consent prior to enrolling a consumer's image in the facial recognition service. Controllers may not deny goods or services, deny entry to a physical place open to the public, or otherwise discriminate against or penalize a consumer who does not consent to the enrollment of the consumer's image. Controllers are permitted to enroll a consumer's image for security or safety purposes without the consumer's consent, if certain requirements are met.

Controllers that use facial recognition services for the purpose of verification, identification, or to make decisions that produce legal effects or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.

Information obtained from or by the use of a facial recognition service may not be received in evidence in any trial, hearing, or other proceeding. Controllers may not knowingly disclose a consumer's personal data obtained from a facial recognition service to law enforcement except when the disclosure is:

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

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

Preemption.

Local governments are preempted from adopting any laws, ordinances, or regulations regarding the processing of personal data by controllers or processors. Local governments are not preempted from adopting any laws, ordinances, or regulations regarding facial recognition.

Liability and Enforcement.

Violations of this act 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 $50,000 for each violation or $100,000 for each intentional violation.

All receipts from the imposition of civil penalties, except for the recovery of costs and attorneys' fees accrued by the Attorney General in enforcing this act, must be deposited into

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

Reports and Research Initiatives.

By July 1, 2022, the Attorney General must submit to the Governor and the Legislature a report evaluating the liability and enforcement provisions, 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 across national and state borders for the purpose of joint data-driven research initiatives. The agreements must provide reciprocal protections that the respective governments agree appropriately safeguard the data.

Substitute Bill Compared to Original Bill:

The substitute bill makes numerous changes to the original bill.

Regarding key definitions and jurisdictional scope, the substitute bill:

- modifies the definition of "child" to apply to a natural person under age 18, rather than age 13;
- modifies the definition of "sale" by specifying several activities that are considered a "sale" and including activities done for a commercial purpose;
- modifies multiple definitions and requirements by removing the word "reasonable" or reasonably such as in the definitions of "authenticate" or "deidentified data" and in the requirement for processors to implement security procedures;
- eliminates the thresholds that a legal entity must meet before the obligations of the bill apply to that entity and instead exempts legal entities that meet certain limits on processing of personal data;
- adds exemptions for personal data used or shared in research, healthcare information regulated by specified federal laws, and personal data collected or processed pursuant to the federal Farm Credit Act;
- specifies that certain data are exempt from the requirements of the bill only to the extent that the collection or processing of that data is in substantial compliance with federal and state laws to which the data are subject and which are specified in the exemptions;
- eliminates the exemption related to controllers that are in compliance with parental consent mechanisms under the federal Children's Online Privacy Protection Act; and
- expires the exemption for data maintained for employment records purposes one year after the effective date of the bill.

Regarding consumer personal data rights, the substitute bill:

- provides that controllers must allow guardians or conservators to exercise consumer personal data rights on behalf of consumers subject to guardianship or conservatorship;

- modifies the right to opt out by providing that a consumer has the right to opt out of the processing of personal data, rather than opt out of the processing for specified purposes; and
- modifies the time limit within which controllers must respond to consumer requests, notify consumers of any extension, or inform consumers of reasons for not taking action on a request from 45 to 21 days.

Regarding responsibilities of controllers and processors, the substitute bill:
- modifies the provision prohibiting discrimination against consumers who exercise personal data rights and allows a controller to offer different prices or rates of service to a consumer who voluntarily participates in a loyalty or reward program;
- prohibits the sale of a consumer's personal data collected as part of a loyalty program to a third-party controller unless specified conditions are met; and
- removes the requirement for controllers to conduct data protection assessments for each of their processing activities and specifies the activities for which controllers must conduct data protection assessments.

Regarding commercial use of facial recognition services, the substitute bill:
- provides that the bill does not preempt local laws or ordinances regarding facial recognition;
- provides that making available an application programming interface for accuracy and bias testing must occur prior to deploying a facial recognition service;
- prohibits controllers from denying goods or services, denying entry to a physical place open to public, or otherwise discriminating against a consumer who does not consent to having the consumer's image enrolled in a facial recognition service;
- requires controllers to test a facial recognition service in operational conditions if using the service for verification, identification, or to make decisions that produce legal effects;
- requires meaningful human review for verification, identification, or decisions that produce legal effects;
- prohibits the use of information obtained from a facial recognition service in any trial or other proceeding;
- exempts from the requirements of the bill voluntary facial recognition services used to verify aviation passengers' identity in connection services regulated by certain federal laws; and
- requires airlines to disclose and obtain a customer consent prior to capturing an image and prohibits airlines from retaining any images captured with the exempt facial recognition service for more than 24 hours.

Regarding liability and enforcement, the substitute bill:
- removes the liability provisions related to the private right of action and the allocation of liability among controllers and processors;
- provides that violations are enforceable under the Consumer Protection Act;
- modifies the civil penalty for violations to not more than $50,000 for each violation; and
- adds a civil penalty of not more than $100,000 for each intentional violation.

Regarding reports and research initiatives, the substitute bill:

- removes the requirement for the Office of Privacy and Data Protection to conduct a study on opt-out technology.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) There are many examples where consumers' personal information is collected without their knowledge, such as when a mobile application collects geolocation information even when the application is not in use. Consumers are beginning to understand how their personal characteristics and experiences are being turned into data for the benefit and profit of the surveillance capitalism economy.

The bill recognizes the robust federal framework under which many financial institutions operate and creates a model for a national comprehensive privacy law. Companies have affirmative obligations with regard to processing personal data, such as conducting risk assessments of all processing activities. The bill provides for strong enforcement by the Attorney General and clarifies that consumers retain their existing ability to sue under the Consumer Protection Act.

Facial recognition creates serious risk of harm to privacy and civil liberties, as well as the risk of bias and discrimination, and it is important to create strong regulation of this technology.

(Opposed) The bill lacks proper protections because it preempts local data privacy and facial recognition laws and does not allow for a private right of action. The long list of exemptions allows businesses many opportunities to override consumer wishes. There needs to be an opt-in, rather than an opt-out, approach to protecting privacy. Clear remedies for individual harms, such as when a person is misidentified and wrongfully arrested, must be integrated into the bill.

Current facial recognition provisions allow for the use of a powerful racially biased and inaccurate technology without applying meaningful restrictions or allowing for a community-driven discussion about whether facial recognition is compatible with our democracy and civil liberties. Facial recognition provisions should be removed from the bill in favor of a moratorium on both public and private use of the technology, particularly in light of recent news about a facial recognition application that scraped over 3 billion images from different websites. History shows that every time a new technology is deployed, it has a disproportionate impact on the most marginalized groups in society. Research shows that facial recognition has been used to perpetuate pseudo-scientific stereotypes to profile certain groups, and it is still very much an open question as to how this technology impacts privacy.

Facial recognition components of the bill are ambiguous and have many loopholes that undermine consumer privacy and diminish vendor accountability. The auditing provisions allow deployment of facial recognition before it has been properly tested for bias and discrimination, and place the burden to show that the technology is biased on the communities most impacted by its use. Notifying consumers as to why a facial recognition service is being used in a public place is a meaningless requirement if consumers are unable to opt out. The use of facial recognition to make decisions that produce legal effects should be prohibited, particularly where the harms of an incorrect decision cannot be remedied retroactively.

(Other) Trust is fundamental in relationship with consumers, and companies must meet reasonable expectations with regard to how personal data is collected and shared. A federal framework is preferred, but federal efforts on a national privacy law move slowly, so Washington can be a leader on the issue.

The bill is a step forward from last year's efforts, but it still needs to be strengthened further or else there will be a lot of room for companies to avoid their responsibilities. The bill maintains interoperability with existing state and federal laws by exempting information regulated by those laws. Requiring substantial compliance for some of these exemptions creates a legal toggle switch; there is no gap in enforcement that necessitates this language in the bill.

A global opt-out should be added in because it is unreasonable to ask consumers to opt out with every company that may be sharing their personal data. The jurisdictional scope provisions are of concern for some small companies with a high volume of transactions. Adding a temporal exemption would help the companies that can easily hit the current thresholds in the bill because they have been in business for decades. The definition of "sale" is of concern because it includes language about other valuable consideration; it is important to get definitions right because simple concepts, such as "sale" or "share," may be interpreted differently by different stakeholders. Current language regarding research restricts or leaves out many responsible researchers. Facial recognition provisions should be removed into a separate bill that does not impose a moratorium on this technology. It is not clear whether third-party loyalty programs would be allowed under the nondiscrimination and loyalty programs provisions.

The Attorney General has limited resources to enforce this bill, and the rights provided in the bill do not have any meaning without a remedy for those individuals whose rights have been violated. There are different ways to provide individual remedies under the bill, including through a private right of action. Concerns about a private right of action could be addressed by adding in a right to cure or allowing for consideration of repetition factors or the depth of culpability. A right to cure may create an incentive for companies to break the law. Additional protections for children and teenagers should be added to the bill.

Persons Testifying: (In support) Representative Kloba, prime sponsor; Ryan Harkins, Microsoft; Alison Phelan, Boeing Employees' Credit Union; Joe Adamack, Northwest Credit Union Association; and Mark Johnson, Washington Retail Association.

(Opposed) Jevan Hutson, William Agnew, Jared Moore, and Christine Geeng, University of Washington; Jennifer Lee, American Civil Liberties Union of Washington; and Stanley Shikuma, Seattle Chapter Japanese American Citizens League.

(Other) Rose Feliciano, Internet Association; Samantha Kersul, TechNet; Anna Powell, Computing Technology Institute Association; Larry Shannon, Washington State Association for Justice; Jaclyn Greenberg, Washington State Hospital Association; Becky Bogard, Life Science Washington; Stuart Halsan, Washington Land Title Association; Trent House, Washington Bankers Association; Joseph Jerome, Common Sense Media; James McMahan, Washington Association Sheriffs and Police Chiefs; Kelsey Finch, Future of Privacy Forum; Maureen Mahoney, Consumer Reports; Bob Battles, Association of Washington Business; Julia Gorton, Washington Hospitality Association; Carolyn Logue, Washington Food Industry Association; and Cliff Webster, Consumer Data Industry Association.

Persons Signed In To Testify But Not Testifying: None.