HOUSE BILL REPORT
HB 1854

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

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

Brief Description: Protecting consumer data.

Sponsors: Representatives Kloba, Hudgins, Slatter, Tarleton, Smith, Ryu, Valdez, Stanford and Pollet.

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 2/12/19, 2/22/19 [DPS];
Appropriations: 2/27/19, 2/28/19 [DP2S(w/o sub ITED)].

Brief Summary of Second Substitute Bill

- Establishes consumer rights with regard to processing of personal information.
- Applies to legal entities that meet specified thresholds.
- Exempts state and local government from the obligations set forth in the act.
- Makes a violation of the act enforceable by the Attorney General under the Consumer Protection Act and subject to civil penalties.
- Provides for a private cause of action after a specified process is completed.
- Creates the Consumer Privacy Account.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 7 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Morris, 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 Boehnke, Assistant Ranking Minority Member; Van Werven.

Staff: Yelena Baker (786-7301).

Background:

Personal information and privacy interests are protected under various provisions of state law. The Washington State Constitution provides that no person shall be disturbed in his private affairs without authority of law. The Public Records Act protects a person's right to privacy under certain circumstances if disclosure of personal information would be highly offensive and is not of legitimate concern to the public.

The 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.

In 2016 the Office of Privacy and Data Protection (OPDP) was created to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection. The primary duties of the OPDP with respect to state agencies include conducting privacy reviews and trainings, coordinating data protection, and articulating privacy principles and best policies.

Summary of Substitute Bill:

Controller and Processor Obligations.

The act applies to legal entities that conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington, and:

- control or process data of 100,000 or more consumers; or
- derive 50 percent of gross revenue from the sale of personal information and process or control personal information of 25,000 or more consumers.

State and local governments and municipal corporations are exempt from the provisions of the act.

Controllers are responsible for meeting the obligations established by the act, and must develop and make publicly available an annual plan for complying with the obligations set forth in the act.

Controllers must be transparent and accountable for their processing of personal data and are required to conduct documented risk assessments. Controllers or processors that use deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments.

Controllers must obtain consent from consumers prior to deploying facial recognition services.

Consumer Rights.

Consumers may require a controller to:
- confirm whether or not personal data concerning the consumer is being processed by the controller;
- provide a copy of the personal data undergoing processing;
- correct inaccurate personal data;
- delete the personal data of the consumer;
- restrict processing of personal data;
- provide the consumer's own personal data that the consumer provided to the controller;
- stop processing the consumer's personal data; and
- not subject the consumer to a decision based solely on profiling.

Enforcement.

Violations of the act are enforceable by the Attorney General under the Consumer Protection Act (CPA). Prior to bringing an action for violations of this chapter, a consumer must provide a controller with a written notice and an opportunity to cure the alleged violations. If the controller does not cure the noticed violations, the consumer must notify the Attorney General of the consumer's intent to bring action, and the Attorney General must either:
- notify the consumer within 30 days that the Attorney General intends to bring an action under the CPA and that the consumer may not proceed with a separate action; or
- refrain from acting within 30 days and allow the consumer to bring an action.

Controllers and processors that violate the provisions of the act are subject to an injunction and a civil penalty of no more than $2,500 for each violation or $7,500 for each intentional violation.

Substitute Bill Compared to Original Bill:

The substitute bill:
- strikes all provisions in the original bill and replaces them, without substantive detail, with provisions related to definitions, responsibilities of controllers and processors, transparency, documented risk assessments, deidentified data, exemptions, and facial recognition;
- modifies jurisdictional scope of the bill by eliminating all exemptions, except for state and local government and municipal corporations;
- specifies that consumers have certain rights with regard to processing of personal data;
- requires controllers to develop and make publicly available an annual compliance plan; and

- modifies enforcement provisions and provides for a private cause of action after a specified process of notifying the controller and the Attorney General is completed.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Substitute Bill: The bill takes effect on July 30, 2021.

Staff Summary of Public Testimony:

(In support) Massive amounts of data are being collected and shared about each person on a daily basis, and the process is largely unnoticed and unobservable for consumers. This bill provides some options giving clarity to consumers and allowing companies to innovate and create the services and opportunities that this sharing and collection of data facilitates.

There is broad support for the concept that a person's data belongs to, and should be controlled by, that person. Stakeholders disagree as to whether this bill is sufficiently protective of the individual rights of privacy or whether it is overly burdensome. This bill empowers consumers to control their data by granting them certain rights that are at the heart of the European Union privacy law. The bill also puts affirmative obligations on companies to start acting like responsible stewards of consumers' personal data by requiring companies to conduct documented risk assessments. The bill also imposes balanced regulation on face recognition technology and would allow that technology to continue developing while addressing legitimate concerns about bias, discrimination, and transparency.

(Opposed) The bill cedes the control to the tech industry and not to the consumers who desperately need to be empowered in this privacy space. Large corporations control data, which are the ultimate source of power and which drive unaccountable data-driven decision-making. Self-policing has not worked. This is a bill written by these large entities, and the choice before the Legislature is whether to continue to allow these companies to exercise outsized power by enacting a bill that gives consumers no meaningful choice, or to insist on a bill that actually makes a difference to the commodification of people's data as practiced by the big tech. The definitions in this bill are watered down and every provision is loaded with loopholes and exemptions that allow companies to use technical means, such as splitting a data set, to avoid having to comply with these provisions. Profiling consumers is openly allowed and everyone should be very concerned about that because that is exactly what these companies are doing.

Provisions related to facial surveillance should be eliminated. The bill contains an underlying assumption that widespread surveillance is simply inevitable and that society must simply deal with its consequences. That is a dangerous assumption and a false one; the best way to prevent a surveillance state is to not build one in the first place. The bill authorizes widespread real-time use of facial surveillance in public spaces and legitimizes profiling for both commercial and criminal justice purpose. The bill does not require independent auditing of facial recognition technology nor does it require that documented

risk assessments be made public. The definition of "facial recognition" is too narrow and fails to capture the practice of affect recognition where an individual's emotional state or state of mind is predicted. This practice has been denounced by scholars as unsupported by science and as a practice that perpetuates racist theories of phrenology. The consent mechanism is particularly insufficient.

The bill contains a prohibition on the use of facial recognition by state and local law enforcement agencies except as pursuant to a warrant or in exigent circumstances. This provision is in conflict with the plain view doctrine and creates a reasonable expectation of privacy in public places. This provision may prohibit the Port of Seattle from using facial recognition to ensure that those on the no-fly list or on the terrorist watch list do not board an airplane.

The bill exempts entities covered by the federal Health Insurance Portability and Accountability Act (HIPAA) but the HIPAA is not the only law that regulates personal health information. Other healthcare entities and datasets should be exempt from the provisions of the bill. The HIPAA protects collection, use, or disclosure of personal health information; this bill only applies to collected data under the HIPAA, which is a step backwards in terms of protection of data.

Title companies process personal data as it relates to sellers and buyers of real estate, and this information is part of the title insurance policy sold to buyers of real estate.

(Other) It is important to make sure that the intent is actually the outcome and that companies can comply. A federal solution to the issue of privacy is preferable to the state-by-state approach. The bill does not offer meaningful protection to Washington consumers and businesses. The bill places responsibility for the protection of data on the first entity to which consumers give their personal data; other entities called "processors" have only limited obligations under the bill. In reality, these processors are large companies with vast market power. The policy choice to regulate controllers but not processors is not consistent with the robust protections of the European Union law and should not be acceptable to Washingtonians.

Enforcement by the Attorney General under the Consumer Protection Act is sufficient; the private right of action should be removed from the bill.

Many small businesses would fall under the scope of this bill.

Unbeknownst to most consumers and health care providers themselves, health information about all consumers is routinely bought and sold in secondary and tertiary markets without the explicit authorization of the individuals. Although these records are deidentified, the availability of additional data sources and the permissible uses of data by these companies have made the entire process highly dysfunctional and unbalanced in favor of data brokers.

Persons Testifying: (In support) Representative Kloba, prime sponsor; Will Saunders, Office of Privacy and Data Protection; and Ryan Harkins, Microsoft.

(Opposed) Shankar Narayan, American Civil Liberties Union of Washington; Jevan Hutson, University of Washington; Lisa Thatcher, Washington State Hospital Association; James McMahan, Washington Association of Sheriffs and Police Chiefs; Cliff Webster, Consumer Data Industry Association; and Stuart Halsan, Washington Land Title Association.

(Other) Rose Feliciano, Internet Association; Michael Transue, Axon; Mark Johnson, Washington Retail Association; Tom McBride, Computing Technology Industry Association; Bob Battles, Association of Washington Business; and Michael DePalma, Hu-manity.co.

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 Innovation, Technology & Economic Development. Signed by 19 members: Representatives Ormsby, Chair; Bergquist, 2nd Vice Chair; Robinson, 1st Vice Chair; Cody, Dolan, Fitzgibbon, Hansen, Hudgins, Jinkins, Macri, Pettigrew, Pollet, Ryu, Senn, Springer, Stanford, Sullivan, Tarleton and Tharinger.

Minority Report: Do not pass. Signed by 11 members: Representatives Stokesbary, Ranking Minority Member; Rude, Assistant Ranking Minority Member; Caldier, Chandler, Dye, Hoff, Kraft, Mosbrucker, Steele, Sutherland and Ybarra.

Minority Report: Without recommendation. Signed by 1 member: Representative MacEwen, Assistant Ranking Minority Member.

Staff: Meghan Morris (786-7119).

Summary of Recommendation of Committee On Appropriations Compared to Recommendation of Committee On Innovation, Technology & Economic Development:

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

- Multiple definitions are added including "controller," "processor," "consumer," and "personal data," among other key terms.
- The provisions apply to natural or legal persons who reside in Washington and jointly own their data.
- The threshold is modified for the provisions to apply to legal entities that conduct business in Washington or intentionally target Washington residents with goods or services.
- The process by which consumers may exercise consumer rights related to processing of personal data is clarified.
- A controller must take action on a consumer request within 30 days of receiving the request, unless an extension is reasonably necessary.
- The controller must notify the consumer of any extension and the reasons for the delay, or the reasons for not taking action on the consumer's request and the possibility for internal review.

- Controllers must provide a privacy notice that includes certain information related to processing of consumers' personal data.
- Specific requirements are outlined regarding the risk assessments that controllers are required to produce in relation to processing of personal data.
- Exemptions for certain controllers or processors are specified.
- Controllers and processors that use facial recognition technology are required to conduct independent testing for bias prior to using the technology and are provided additional requirements with regard to the use of facial recognition technology by controllers and processors.
- State and local governments are prohibited from using facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces without a court order or absent imminent danger or risk of death or serious injury to a person.
- The Consumer Privacy Account is created. Receipts from civil penalties shall be deposited into the account to fund the Office of Privacy and Data Protection (OPDP).
- The OPDP must conduct an analysis on the public sector use of facial recognition and to report its findings to the Legislature by September 30, 2023.
- The OPDP, in consultation with the Attorney General, must develop by rule any exceptions necessary to comply with state or federal law, clarify definitions where necessary, and create exemption eligibility requirements for small businesses and research institutions.
- The bill is null and void unless funded in the budget.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Second Substitute Bill: The bill takes effect on July 30, 2021. However, the bill is null and void unless funded in the budget.

Staff Summary of Public Testimony:

(In support) None.

(Opposed) There should be a federal solution rather than a state-by-state approach. Washington residents should have the same level of robust privacy safeguards as the European Union (EU) residents. The EU offers a data protection system that applies to all entities that touch consumer data through the Internet, and this bill does not. Washington should give small businesses the tools they need to provide the same level of data protection. The health care industry is already heavily regulated, and needs a clear exemption. Clarification should be provided that use of consumer data is allowed when in compliance with specific federal laws. Those who are complying with the provisions of the Children Online Privacy Protection Act should also be exempted. Schools are looking to use facial recognition technology in a layered security strategy, which should be allowed under the bill. The warrant provisions related to law enforcement use of facial recognition technology are unconstitutional and unenforceable.

(Other) There is already robust federal oversight over financial data, such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act; this legislation should recognize that

fact. Proprietary and trade secret information should not be divulged. There should be an exemption in reference to body cameras and facial recognition technology as it relates to law enforcement. The definition of data covered should include the full range of data that is stored with modern data practices. Companies should be able to get advice from their regulator in order to comply.

Persons Testifying: (Opposed) Mark Johnson, Washington Retail; Lisa Thatcher, Washington State Hospital Association; Brad Tower, The Toy Association and Community Bankers of Washington; Cliff Webster, Consumer Data Industry Association; Mark Streuli, Motorola Solutions; and James McMahan, Washington Association of Sheriffs and Police Chiefs.

(Other) Trent House, Washington Bankers Association; Michael Transue, Axon Enterprises; and Ryan Harkins, Microsoft.

Persons Signed In To Testify But Not Testifying: None.