SENATE BILL REPORT
SB 5062

As of January 14, 2021

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

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

Sponsors: Senators Carlyle, Nguyen, Billig, Darneille, Das, Dhingra, Holy, Hunt, Lovelett, Mullet, Pedersen, Salomon, Sheldon, Wellman and Wilson, C..

Brief History:
Committee Activity: Environment, Energy & Technology: 1/14/21.

Brief Summary of Bill

- Provides Washington residents with the consumer personal data rights of access, correction, deletion, data portability, and opt out of the processing of personal data for specified purposes.
- Specifies the thresholds a legal entity must satisfy for the requirements set forth in this act to apply.
- Identifies controller responsibilities such as transparency, purpose specification, and data minimization.
- Requires controllers to conduct data protection assessments under certain conditions.
- Authorizes sole attorney general enforcement under the Consumer Protection Act.
- Regulates the processing of data collected for certain contact tracing purposes.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Staff: Angela Kleis (786-7469)

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.

Background: Federal. The Federal Trade Commission (FTC) has been the chief federal agency on privacy policy and enforcement since the 1970s when it began enforcing the Fair Credit Reporting Act, one of the first federal privacy laws. The FTC has broad authority to prohibit unfair and deceptive practices. In general, the FTC enforces sector-specific privacy regulations.

California. In 2018, California enacted the California Consumer Privacy Act (CCPA), which took effect in 2020. The CCPA regulates the collection, use, and sharing of personal information and provides California residents with certain rights such as access and opt out of the sale of personal information to third parties. In November 2020, California residents approved a ballot initiative titled the California Privacy Rights Act (CPRA), which amends many provisions of the CCPA. For example, CPRA expands the opt out right to include the sharing of personal information and establishes a new agency to be the regulatory and enforcement entity for privacy protections. CPRA takes effect in January 2023.

Washington State. *Privacy Regulations in General.* Personal information and privacy interests are protected under various provisions of state law, such as biometric identifiers and personal information–notice of security breaches. The Washington State Constitution provides that no person is disturbed in their private affairs without authority of law.

State Privacy Office. The Office of the Chief Information Officer (OCIO) has primary duties related to information technology for state government, which include establishing statewide enterprise architecture and standards for consistent and efficient operation. Within the OCIO, the Office of Privacy and Data Protection (OPDP) serves as a central point of contact for state agencies on policy matters involving data privacy and data protection. The OPDP also serves as a resource to local governments and the public on data privacy and protection concerns.

Washington Consumer Protections. 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 (AG) 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.

Contact Tracing. Local health departments, with the support of the Department of Health (DOH) and its partners, perform case investigations and contact tracing to help slow and prevent the spread of infectious diseases like COVID-19. These practices have been used for decades and entail an interviewer reaching out to persons who have tested positive for infectious disease, asking them pre-approved questions, entering information into secure systems, and connecting people with appropriate resources. Information collected during these interviews is only used by public health agencies.

In December 2020, DOH launched exposure notifications technology known as WA Notify. This is a new tool that works through smartphones, without sharing any personal information, to notify users if they may have been exposed to COVID-19. It is private and does not know or track the identity of an individual or where they go. Notifications have a link to information about what to do next to protect themselves and others. Notifications do not contain any information about who tested positive or where the exposure may have happened.

Summary of Bill: Consumer Personal Data–Private Sector. *Rights.* A consumer has the following rights regarding their personal data:

- access;
- correction;
- deletion;
- obtaining personal data they provided to the controller in a portable format; and
- opt out of the processing of their personal data for purposes of (1) targeted advertising, (2) the sale of personal data, or (3) profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

Consumers may exercise these rights at any time. In the case of processing of personal data concerning a known child or a consumer subject to protective arrangements, the parent or legal guardian of the known child or the conservator of the consumer shall exercise these rights on their behalf.

Jurisdictional Scope. This act applies to legal entities conducting business in Washington or producing products or services targeted to Washington residents, and:

- controlling or processing personal data of 100,000 or more consumers during a calendar year; or
- deriving 25 percent of gross revenue from the sale of personal data and processing or controlling personal data of 25,000 or more consumers.

This act does not apply to state agencies, legislative agencies, local governments, tribes, municipal corporations, personal data regulated by certain federal and state laws, or data maintained for employment records purposes.

Responding to Consumer Requests. A controller must comply with a request to opt out of processing no later than 15 days of receipt of the request.

A controller must inform a consumer of any action, including an extension, taken on a request to access, delete, correct, or obtain data in a portable format within 45 days of receipt of the request. This timeframe may be extended once for an additional 45 days. If a controller does not take action on a request, the controller must inform the consumer within 45 days of receipt of the request with the reasons for not taking action and instructions on how to appeal the decision with the controller. Controllers must establish an internal

process for consumers to appeal a refusal to take action.

The controller must provide information free of charge, up to twice annually, to the consumer. When requests from a consumer are manifestly unfounded or excessive, the controllers may either charge a reasonable administrative fee or refuse to act on the request. A controller is not required to comply with a request to exercise a consumer personal data right if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request additional information.

Responsibility According to Role. Controllers and processors are responsible for meeting set obligations. Processors must adhere to instructions of the controller and assist controllers in meeting set obligations. Notwithstanding the instructions of the controller, a processor must ensure the confidentiality of the processing of personal data and engage with a subcontractor only after certain requirements are met.

Processing by a processor is governed by a contract between the controller and the processor that is binding on both parties. Contractual requirements are specified.

Responsibilities of Controllers. Controller responsibilities are specified including transparency, data minimization, purpose specification, avoiding secondary use, nondiscrimination, and antiretaliation. Controllers must obtain consumer consent to process sensitive data.

Processing Deidentified Data or Pseudonymous Data. Controllers or 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. The consumer rights identified in this act do not apply to pseudonymous data in cases where the controller is able to demonstrate it is not in a position to identify the consumer. A controller or processor that uses deidentified data or pseudonymous data must monitor compliance with any contractual commitments.

Data Protection Assessments. Controllers must conduct and document a data protection assessment (assessment) of each of the following activities involving personal data:

- processing of personal data for purposes of targeted advertising, the sale of personal data, and profiling, where such profiling presents reasonably foreseeable risks to consumers such as unfair impact or financial, physical, or reputational injury;
- processing of sensitive data; and
- any processing activities involving personal data that present a heightened risk of harm to consumers.

The AG may request, in writing, that a controller disclose any assessment relevant to an investigation conducted by the AG. Assessments are confidential and exempt from public inspection.

Assessments conducted by a controller in compliance with other laws or regulations may qualify if they have a similar scope and effect.

Limitations and Applicability. Several exemptions to the obligations imposed on controllers or processors are specified such as complying with federal, state, or local laws; providing a service specifically requested by a consumer; or engaging in research that adheres to privacy laws and is monitored by an independent oversight entity.

If a controller processes personal data pursuant to a specified exemption, the controller bears the burden of demonstrating such processing qualifies for the exemption and complies with specified requirements. Personal data processed pursuant to an exemption may be processed solely to the extent that such processing is:

- necessary for the listed purpose;
- limited to what is necessary relative to the specified purpose; and
- subject to security measures to protect the confidentiality of the personal data and to reduce reasonably foreseeable risks of harm to consumers.

Private Right of Action. A violation of this chapter may not serve as the basis for a private right of action under this chapter or any other law. Rights possessed by consumers as of July 1, 2020, under the CPA or other laws are not altered.

Enforcement. This chapter may be enforced solely by the AG under the CPA. If a controller or processor violates this act, prior to filing a complaint, the AG must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the AG alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the AG believes the controller or processor has failed to cure any alleged violation, the AG may bring an action as provided under this chapter.

A controller or processor found in violation of this chapter is subject to a civil penalty up to $7,500 for each violation. In actions brought under this chapter, the state is entitled to recover, in addition to prescribed penalties, the costs of investigation, including reasonable attorneys' fees.

Consumer Privacy Account. The Consumer Privacy Account is created. All receipts from the imposition of civil penalties, except for the recovery of costs and attorneys' fees accrued during enforcement, must be deposited into the Consumer Privacy Account. Expenditures from the account may only be used for the purposes of the OPDP.

Preemption. This act supersedes and preempts laws or the equivalent adopted by any local entity regarding the processing of personal data by controllers or processors. Laws, ordinances, or regulations regarding the processing of personal data by controllers or processors adopted by any local entity prior to July 1, 2020, are not superseded or preempted.

Severability Clause. If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to the other persons or circumstances is not affected.

Privacy Office Report. The OPDP, in collaboration with the Office of the Attorney General, shall research and examine existing analysis on the development of technology, such as a browser or global device setting, indicating a consumer's affirmative, freely given, and unambiguous choice to opt out of certain processing. A contract study is not required. A report of findings and specific recommendations must be submitted to the Governor and the Legislature by December 1, 2022.

Data Processed for Contact Tracing Purposes–Private Sector. *Prohibitions.* It is unlawful for a controller or processor to:

- process covered data for a covered purpose unless they provide a consumer with the required privacy notice and obtain consumer consent;
- disclose covered data to federal, state, or local law enforcement;
- sell any covered data; or
- share covered data with another controller, processor, or third party unless such sharing is covered by a contract.

Rights. A consumer has the following rights regarding the processing of covered data for a covered purpose:

- opt out;
- access;
- correction; and
- deletion.

Responsibilities of Controllers. Controller responsibilities are specified including transparency, data minimization, purpose specification, and nondiscrimination. Controllers must delete or deidentify covered data when it is no longer being used for the covered purpose.

Limitations and Applicability. The obligations imposed on controllers or processors under this chapter do restrict their ability to comply with federal, state, or local laws; or engage in research that adheres to privacy laws and is monitored by an independent oversight entity. This chapter does not apply to certain data governed by federal or state law or employment records.

Provisions Similar to Consumer Personal Data–Private Sector. Several provisions related to consumer personal data also apply to the processing of covered data processed for a covered purpose including exercising consumer rights, responding to requests, responsibilities according to role, private right of action, enforcement, preemption, and severability clause. Data type terminology is different in order to reflect applicable definitions.

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

Covered purpose means processing of covered data concerning a consumer for the purposes of detecting symptoms of an infectious disease, enabling the tracking of a consumer's contact with other consumers, or specific locations to identify, in an automated fashion, whom consumers have come into contact with, or digitally notifying, in an automated manner, a consumer who may have become exposed to an infectious disease, or other similar purposes directly related to a state of emergency declared by the Governor.

Data Process for Contact Tracing Purposes–Public Sector. *Prohibitions.* It is unlawful for a controller or processor to:

- process technology-assisted contact tracing (TACT) information unless they provide a consumer with the required privacy notice and obtain consumer consent;
- disclose TACT information to federal, state, or local law enforcement;
- sell any TACT information; or
- share TACT information with another controller, processor, or third party unless such sharing is covered by a contract or data-sharing agreement.

Responsibilities of Controllers. Controller responsibilities are specified including transparency, data minimization, purpose specification, and nondiscrimination. Controllers must delete or deidentify covered data when it is no longer being used for the covered purpose.

Limitations and Applicability. The obligations imposed on controllers or processors under this chapter do restrict their ability to comply with federal, state, or local laws; or engage in research that adheres to privacy laws and is monitored by an independent oversight entity.

Enforcement. Any individual injured by a violation of this chapter may institute a civil action to recover damages. Any controller that violates, proposes to violate, or has violated this chapter may be enjoined.

Liability. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability must be allocated among the parties according to principles of comparative fault.

Definitions. TACT means the use of a digital application or other electronic or digital platform capable of independently transmitting information and if offered to individuals for the purpose of notifying individuals who may have had contact with an infectious person through data collection and analysis as a means of controlling the spread of a communicable disease.

TACT information means any information, data, or metadata received through TACT.

Expiration. The provisions related to data processed for public sector contact tracing purposes expire June 30, 2024.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: The bill contains several effective dates. Please refer to the bill.

Staff Summary of Public Testimony: PRO: Consumers only have rights that are granted to them by businesses. The bill provides new rights and gives consumers more control over the handling of their data. By providing a regulatory framework for the processing of data, consumers are provided data protections, businesses may advance services and operate with increased predictability, and public confidence and trust will be fostered. Contact tracing provisions are needed to build public confidence in using tools to help stop the spread of COVID-19.

CON: This bill does not provide meaningful consumer protection regulations. People need to be able to bring a private right of action, which this bill explicitly prohibits, in order to protect their privacy rights and hold businesses accountable. This approach protects businesses rather than consumers by providing several exemptions. Financial information should be included. This bill fails to protect sensitive data shared by children in schools. The bill should include protections for teenagers. Contact tracing provisions should be addressed in a separate bill. An opt-in framework provides better protections than the opt-in provisions of the bill. Major platforms are carved out of the bill. Local jurisdictions should be able to enact stronger privacy laws.

OTHER: This bill reflects all of the hard work that has gone into this issue over several years and represents a compromise amongst various stakeholders. We are concerned that the definition of targeted advertising is confusing. We recommend a couple of measures that will help consumers exercise their rights such as recognizing global opt out mechanisms and authorizing delegated authority. With regards to enforcement, we have concerns with the cure period. This bill provides tools needed for enforcement. Compliance is burdensome; nonprofits should be exempt from these requirements just as they are in California. We have concerns that the provisions regarding loyalty programs might invalidate some partnerships.

Persons Testifying: PRO: Senator Reuven Carlyle, Prime Sponsor; Molly Jones, Washington Technology Industry Association; Ryan Harkins, Microsoft Corporation; Derrick Morton, FlowPlay.

CON: Jennifer Lee, American Civil Liberties Union of Washington; Gregg Brown, citizen, Former Microsoft Privacy Standards; Brianna Auffrey, Council on American-Islamic Relations of Washington; Susan Grant, Consumer Federation of America; Emilie St-Pierre, Future Ada; Cynthia Spiess, citizen, Independent Security Expert; Jon Pincus, Indivisible+ Washington; Stephanie Hager, citizen; Cheri Kiesecker, Parent Coalition for Student Privacy.

OTHER: Mark Johnson, Washington Retail; Rose Feliciano, Internet Association; Maureen Mahoney, Consumer Reports; Joseph Jerome, Common Sense Media; Yasmin Trudeau, Washington State Office of the Attorney General; Kristen Knauf, American Heart Association; Robert Battles, Association of Washington Business; Julia Gorton, Washington Hospitality Association; Samantha Kersul, TechNet; Carolyn Logue, Washington Food Industry Association; Larry Shannon, Washington State Association for Justice; Ryan Tack-Hooper, Washington State Association for Justice.

Persons Signed In To Testify But Not Testifying: No one.