SECOND SUBSTITUTE HOUSE BILL 1854

State of Washington 66th Legislature 2019 Regular Session

By House Appropriations (originally sponsored by Representatives Kloba, Hudgins, Slatter, Tarleton, Smith, Ryu, Valdez, Stanford, and Pollet)

READ FIRST TIME 03/01/19.

AN ACT Relating to the management and oversight of personal data; amending RCW 43.105.369; adding a new section to chapter 9.73 RCW; adding a new chapter to Title 19 RCW; creating new sections; prescribing penalties; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and cited as the Washington privacy act.

NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS. (1) The legislature finds that:

(a) Washington explicitly recognizes its people's right to privacy under Article I, section 7 of the state Constitution.

(b) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. The protection of individual privacy and freedom in relation to the processing of personal data requires the recognition of the principle of joint ownership of personal data between consumers and controllers that process the data.

(2) To preserve trust and confidence that personal data will be protected appropriately, the legislature recognizes that with regard

to processing of personal data, Washington consumers have the rights to:

(a) Confirm whether or not personal data is being processed by a controller;

(b) Obtain a copy of the personal data undergoing processing;

(c) Correct inaccurate personal data;

(d) Obtain deletion of personal data;

(e) Restrict processing of personal data;

(f) Be provided with any of the consumer's personal data that the consumer provided to a controller;

(g) Object to processing of personal data; and

(h) Not be subject to a decision based solely on profiling.

NEW SECTION. **Sec. 3.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity.

(2) "Business associate" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(3) "Business purpose" means the processing of personal data for the controller's or its processor's operational purposes, or other notified purposes, provided that the processing of personal data must be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected. Business purposes include:

(a) Auditing related to a current interaction with the consumer and concurrent transactions including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(b) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

(c) Identifying and repairing errors that impair existing or intended functionality;

(d) Short-term, transient use, provided the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction including, but not limited to, the contextual customization of ads shown as part of the same interaction;

(e) Maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

(f) Undertaking internal research for technological development; or

(g) Authenticating a consumer's identity.

(4) "Child" means any natural person under thirteen years of age.

(5) "Consent" means a clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

(6) "Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

(7) "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(8) "Covered entity" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(9)(a) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(b) Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker.

(c) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier, does not qualify the business as a data broker.

(10) "Deidentified data" means:

(a) Data that cannot be linked to a known natural person without additional information kept separately; or

(b) Data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

(11) "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

(12) "Direct marketing" means communication with a consumer for advertising purposes or to market goods.

(13) "Facial recognition" means technology that analyzes facial features for the unique personal identification of natural persons in still or video images. "Facial recognition" means both:

(a) The automated or semiautomated process by which a person is identified or attempted to be identified based on the characteristics of their face, including identification of known or unknown individuals or groups; and

(b) The automated or semiautomated process by which the characteristics of an individual's face are analyzed to determine the individual's sentiment, state of mind, or other propensities.

(14) "Health care facility" has the same meaning as in RCW 70.02.010.

(15) "Health care information" has the same meaning as in RCW 70.02.010.

(16) "Health care provider" has the same meaning as in RCW 70.02.010.

(17) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, or specific geolocation data.

(18) "Legal effects" means, without limitation, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and other similarly significant effects.

(19) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data.

(20) "Process" or "processing" means any collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(21) "Processor" means a controller that processes personal data or a natural or legal person that processes personal data on behalf of the controller.

(22) "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(23) "Protected health information" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(24) "Publicly available information" means information that is lawfully made available from federal, state, or local government records.

(25) "Request" means the process through which a consumer may submit a request to exercise a right or rights set forth in this chapter, and by which a controller can reasonably authenticate the request and the consumer making the request using reasonable means.

(26) "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

(27) "Sale," "sell," or "sold" means the exchange of personal data for consideration by the controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties.

(28) "Sensitive data" means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; or (c) the personal data of a known child.

(29) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across

nonaffiliated web sites, applications, or online services to predict user preferences or interests.

(30) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, or an affiliate of the processor of the controller.

NEW SECTION. **Sec. 4.** JURISDICTIONAL SCOPE. (1) This chapter applies to natural or legal persons who reside in Washington and jointly own their personal data.

(2) This chapter applies to legal entities that conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) Controls or processes personal data of one hundred thousand consumers or more; or

(b) Derives over twenty-five percent of gross revenue from the sale of personal data and processes or controls personal data of ten thousand consumers or more.

(3) This chapter does not apply to:

(a) State and local governments; or

(b) Municipal corporations.

NEW SECTION. **Sec. 5.** RESPONSIBILITY ACCORDING TO ROLE. (1) Controllers are responsible for meeting the obligations established under this chapter.

(2) Processors are responsible under this act for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter.

(3) Processing by a processor is governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

NEW SECTION. **Sec. 6.** CONSUMER RIGHTS. (1) A consumer may exercise any of the consumer rights set forth in section 2 of this act by submitting to a controller a request that specifies which rights the consumer wishes to exercise.

(2) Upon receiving a consumer request, a controller must:

(a) Confirm whether or not the consumer's personal data is being processed by the controller, including whether such personal data is sold to data brokers, and, where the consumer's personal data is being processed by the controller, provide access to such personal data that the controller maintains in identifiable form;

(b) Provide a copy of the consumer's personal data that is undergoing processing and that the controller maintains in identifiable form;

(c) Correct the consumer's inaccurate personal data that the controller maintains in identifiable form;

(d) Complete the consumer's incomplete personal data, including by means of providing a supplementary statement where appropriate;

(e) Delete the consumer's personal data that the controller maintains, including personal data that:

(i) Has been unlawfully processed;

(ii) Must be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject; or

(iii) Has been disclosed by the controller to third parties, including data brokers that received the consumer's personal data through a sale;

(f) Take reasonable steps to inform other controllers of which the controller is aware, and which are processing the consumer's personal data they received from the controller or are processing such personal data on behalf of the controller, that the consumer has requested the other controllers delete any copy of or links to the consumer's personal data;

(g) Restrict processing of the consumer's personal data if the purpose for which the personal data is being processed is: (i) Inconsistent with a purpose for which the personal data was collected; (ii) inconsistent with a purpose disclosed to the consumer at the time of collection or authorization; or (iii) unlawful;

(h) Inform the consumer before any existing restriction of processing is lifted;

(i) Provide to the consumer any personal data concerning the consumer that such consumer has provided to the controller;

(j) Stop processing personal data of the consumer who objects to such processing, including the selling of the consumer's personal data to third parties for purposes of direct marketing or targeted advertising;

(k) Inform the consumer about third-party recipients of the consumer's personal data, including third parties that received the data through a sale; or

(l) Communicate a consumer's objection to processing to third parties to whom the controller sold the consumer's personal data and who must honor objection requests received from the controller.

(3) A controller must take action on a consumer's request without undue delay and within thirty days of receiving the request. The request fulfillment period may be extended by sixty additional days where reasonably necessary, taking into account the complexity of the request.

(4) Within thirty days of receiving a consumer request, a controller must inform the consumer about:

(a) Any fulfillment period extension, together with the reasons for the delay; or

(b) The reasons for not taking action on the consumer's request and any possibility for internal review of the decision by the controller.

(5) A controller must communicate any correction, deletion, or restriction of processing carried out pursuant to a consumer request to each third party to whom the controller knows the consumer's personal data has been disclosed, including third parties that received the data through a sale.

(6) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, the controller may refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(7) Where a controller has reasonable doubts concerning the identity of the consumer making a request under this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

(8) Requests for personal data under this section must be without prejudice to the other rights granted in this chapter.

(9) The rights provided in this section must not adversely affect the rights of others.

(10) All policies adopted and used by a controller to comply with this section must be publicly available on the controller's web site and included in the controller's online privacy policy.

NEW SECTION. **Sec. 7.** TRANSPARENCY. (1) Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes:

(a) The categories of personal data collected by the controller;

(b) The purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) The rights that consumers may exercise pursuant to section 6 of this act, if any;

(d) The categories of personal data that the controller shares with third parties, if any;

(e) The categories of third parties, if any, with whom the controller shares personal data; and

(f) The process by which a consumer may request to exercise the rights under section 6 of this act, including a process by which a consumer may appeal a controller's action with regard to the consumer's request.

(2) If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted advertising, it must disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.

NEW SECTION. **Sec. 8.** COMPLIANCE. (1) Controllers must develop and make publicly available an annual plan for complying with the obligations under this chapter.

(2) A controller that has developed a compliance plan for the European general data protection regulation 2016/679 may use that plan for purposes of subsection (1) of this section.

(3) Controllers may report metrics on their public web site to exemplify and support their compliance plans.

NEW SECTION. **Sec. 9.** RISK ASSESSMENTS. (1) Controllers must produce a risk assessment of each of their processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. The risk assessments must take into account the:

(a) Type of personal data to be processed by the controller;

(b) Extent to which the personal data is sensitive data or otherwise sensitive in nature; and

(c) Context in which the personal data is to be processed.

(2) Risk assessments conducted under subsection (1) of this section must:

(a) Identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce risks; and

(b) Factor in the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(3) If the risk assessment conducted under subsection (1) of this section determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer. To the extent the controller seeks consumer consent for processing, consent must be as easy to withdraw as to give.

(4) Processing for a business purpose is permissible unless: (a) It involves the processing of sensitive data; (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards; or (c) consent was not given.

(5) The controller must make the risk assessment available to the attorney general upon request. Risk assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW.

NEW SECTION. **Sec. 10.** DEIDENTIFIED DATA. A controller or processor that uses 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.

NEW SECTION. **Sec. 11.** EXEMPTIONS. (1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

(a) Engage in processing that is necessary for reasons of public health interest, where the processing: (i) Is subject to suitable and specific measures to safeguard consumer rights; and (ii) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(b) Engage in processing that is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;

(c) Comply with federal, state, or local laws, rules, or regulations;

(d) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(e) Establish, exercise, or defend legal claims;

(f) Authenticate identities;

(g) Safeguard intellectual property rights;

(h) Prevent, detect, or respond to security incidents;

(i) Protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that illegal activity;

(j) Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

(k) Protect the vital interests of the consumer or of another natural person;

(l) Perform a task carried out in the public interest or in the exercise of official authority vested in the controller;

(m) Process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or

(n) Assist another controller, processor, or third party with any of the activities under this subsection.

(2) The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under Washington law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Washington law as part of a privileged communication.

(3) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter is not in violation of this chapter, including under section 13 of this act, if the recipient processes such personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor is likewise not liable under this chapter, including under section 13 of this act, for the obligations of a controller or processor to which it provides services.

(4) This chapter does not require a controller or processor to do the following:

(a) Reidentify deidentified data;

(b) Retain, link, or combine personal data concerning a consumer that it would not otherwise retain, link, or combine in the ordinary course of business;

(c) Comply with a request to exercise any of the rights under section 6 of this act if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

(5) Obligations imposed on controllers and processors under this chapter do not:

(a) Adversely affect the rights or freedoms of any persons; or

(b) Apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

NEW SECTION. **Sec. 12.** FACIAL RECOGNITION. (1) Prior to using facial recognition technology, controllers and processors must verify, through independent third-party testing or auditing, that no statistically significant variation occurs in the accuracy of the facial recognition technology on the basis of race, skin tone, ethnicity, gender, or age of the individuals portrayed in testing images.

(2) Controllers may not use facial recognition for profiling and must employ meaningful human review prior to making final decisions based on the use of facial recognition technology where final decisions produce legal effects concerning consumers.

(3) Processors that provide facial recognition services must provide documentation that includes general information that explains the capabilities and limitations of the technology in terms that customers and consumers can understand.

(4) Processors that provide facial recognition services must prohibit, in the contract required by section 5 of this act, the use of such facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.

(5) Controllers must obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public. The placement of conspicuous notice in physical premises that clearly conveys that facial recognition services are being used does not constitute a consumer's consent to the use of facial recognition services when that consumer enters a premises that have such a notice. Active, informed consumer consent is required before facial recognition may be used or any data resulting from the use of facial recognition may be processed.

(6) Providers of commercial facial recognition services that make their technology available as an online service for developers and customers to use in their own scenarios must make available an application programming interface or other technical capability, chosen by the provider, to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of those facial recognition services for accuracy and unfair bias. Providers must track and correct instances of bias identified by this independent testing.

(7) Controllers, processors, and providers of facial recognition services must notify consumers if an automated decision system makes decisions affecting the constitutional or legal rights, duties, or privileges of any Washington resident.

NEW SECTION. **Sec. 13.** 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, unless liability is otherwise allocated by contract among the parties.

NEW SECTION. **Sec. 14.** ENFORCEMENT. (1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

(2) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter.

(3) Prior to bringing an action for violations of this chapter, a consumer must provide a controller with a written notice identifying the specific provisions of this chapter that the consumer alleges have been or are being violated. In the event a cure is possible and the controller does not cure the noticed violation within thirty days, the consumer must notify the attorney general of the consumer's intent to bring an action.

(4) Upon receiving such notice, the attorney general must either:

(a) Notify the consumer within thirty days that the attorney general intends to bring an action under subsections (1) and (2) of this section and that the consumer may not proceed with a separate action; or

(b) Refrain from acting within thirty days and allow the consumer to bring an action.

(5) Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars for each violation or seven thousand five hundred dollars for each intentional violation.

(6) The consumer privacy account is created in the state treasury. All receipts from the imposition of civil penalties pursuant to an action by the attorney general under this chapter must be deposited into the account. Moneys in the account may be spent only after appropriation. Expenditures from the account may be used only to fund the office of privacy and data protection as established under RCW 43.105.369.

Sec. 15. RCW 43.105.369 and 2016 c 195 s 2 are each amended to read as follows:

(1) The office of privacy and data protection is created within the office of the state chief information officer. The purpose of the office of privacy and data protection is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection.

(2) The director shall appoint the chief privacy officer, who is the director of the office of privacy and data protection.

(3) The primary duties of the office of privacy and data protection with respect to state agencies are:

(a) To conduct an annual privacy review;

(b) To conduct an annual privacy training for state agencies and employees;

(c) To articulate privacy principles and best practices;

(d) To coordinate data protection in cooperation with the agency; and

(e) To participate with the office of the state chief information officer in the review of major state agency projects involving personally identifiable information.

(4) The office of privacy and data protection must serve as a resource to local governments and the public on data privacy and protection concerns by:

(a) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and

(b) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.

(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These performance measures must include, but are not limited to, the following:

(a) The number of state agencies and employees who have participated in the annual privacy training;

(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;

(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and

(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

(6) Within one year of June 9, 2016, the office of privacy and data protection must submit to the joint legislative audit and review committee for review and comment the performance measures developed under subsection (5) of this section and a data collection plan.

(7) The office of privacy and data protection shall submit a report to the legislature on the: (a) Extent to which telecommunications providers in the state are deploying advanced telecommunications capability; and (b) existence of any inequality in access to advanced telecommunications infrastructure experienced by residents of tribal lands, rural areas, and economically distressed communities. The report may be submitted at a time within the discretion of the office of privacy and data protection, at least once every four years, and only to the extent the office of privacy and data protection is able to gather and present the information within existing resources.

(8) The office of privacy and data protection must conduct an analysis on the public sector use of facial recognition. By September 30, 2022, the office of privacy and data protection must submit a report of its findings to the appropriate committees of the legislature.

(9) The office of privacy and data protection, in consultation with the attorney general, must by rule (a) establish any exceptions to this chapter necessary to comply with state or federal law by the effective date of this section and as necessary thereafter, (b) clarify definitions of this chapter as necessary, and (c) create exemption eligibility requirements for small businesses and research institutions.

NEW SECTION. **Sec. 16.** A new section is added to chapter 9.73 RCW to read as follows:

(1) State and local government agencies may not use facial recognition technology to engage in ongoing surveillance of specified individuals in public places, unless such a use is in support of law enforcement activities and either: (a) A court issued a warrant based on probable cause to permit the use of facial recognition technology for that surveillance during a specified time frame; or (b) there is an emergency involving imminent danger or risk of death or serious injury to a person.

(2) For purposes of this section, "facial recognition" has the same meaning as in section 3 of this act.

NEW SECTION. **Sec. 17.** PREEMPTION. This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by controllers or processors.

NEW SECTION. **Sec. 18.** Sections 1 through 14 and 17 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 19.** If specific funding for the purposes of this act, referencing this act by bill or chapter number, is not provided by June 30, 2019, in the omnibus appropriations act, this act is null and void.

NEW SECTION. **Sec. 20.** 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 other persons or circumstances is not affected.

NEW SECTION. **Sec. 21.** If any provision of this act is found to be in conflict with federal or state law or regulations, the conflicting provision of this act is declared to be inoperative.

NEW SECTION. **Sec. 22.** This act takes effect July 30, 2021.

--- END ---