S-6225.1

SECOND SUBSTITUTE SENATE BILL 6281

State of Washington 66th Legislature 2020 Regular Session

By Senate Ways & Means (originally sponsored by Senators Carlyle, Nguyen, Rivers, Short, Sheldon, Wellman, Lovelett, Das, Van De Wege, Billig, Randall, Pedersen, Dhingra, Hunt, Salomon, Liias, Mullet, Wilson, C., Frockt, Cleveland, and Keiser)

READ FIRST TIME 02/07/20.

AN ACT Relating to the management and oversight of personal data; adding a new chapter to Title 19 RCW; 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 the people of Washington regard their privacy as a fundamental right and an essential element of their individual freedom. Washington's Constitution explicitly provides the right to privacy, and fundamental privacy rights have long been and continue to be integral to protecting Washingtonians and to safeguarding our democratic republic.

(2) Ongoing advances in technology have produced an exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed, which presents both promise and potential peril. The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society; however, it has also created risks to privacy and freedom. The unregulated and unauthorized use and disclosure of personal

information and loss of privacy can have devastating impacts, ranging from financial fraud, identity theft, and unnecessary costs, to personal time and finances, to destruction of property, harassment, reputational damage, emotional distress, and physical harm.

(3) Given that technological innovation and new uses of data can help solve societal problems and improve quality of life, the legislature seeks to shape responsible public policies where innovation and protection of individual privacy coexist. The legislature notes that our federal authorities have not developed or adopted into law regulatory or legislative solutions that give consumers control over their privacy. In contrast, the European Union's general data protection regulation has continued to influence data privacy policies and practices of those businesses competing in global markets. In the absence of federal standards, Washington and other states across the United States are analyzing elements of the European Union's general data protection regulation to enact state-based data privacy regulatory protections.

(4) With this act, Washington state will be among the first tier of states giving consumers the ability to protect their own rights to privacy and requiring companies to be responsible custodians of data as technological innovations emerge. This act does so by explicitly providing consumers the right to access, correction, and deletion of personal data, as well as the right to opt out of the collection and use of personal data for certain purposes. These rights will add to, and not subtract from, the consumer protection rights that consumers already have under Washington state law.

(5) Additionally, this act imposes affirmative obligations upon companies to safeguard personal data and provide clear, understandable, and transparent information to consumers about how their personal data are used. It strengthens compliance and accountability by requiring data protection assessments in the collection and use of personal data. Finally, it empowers the state attorney general to obtain and evaluate a company's data protection assessments, to impose penalties where violations occur, and to prevent against future violations.

(6) The legislature also encourages the state office of privacy and data protection to monitor the development of universal privacy controls that communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data concerning the consumer for the purposes of targeted advertising, the

sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning the consumer or similarly significant effects concerning consumers.

(7) The legislature recognizes the unique business needs of institutions of higher education and nonprofit corporations. However, these entities control and process an extraordinary amount of personal data and consumers should be afforded the rights provided by this act regarding personal data. Therefore, it is the intent of the legislature to delay the date of application for these entities by three years in order to provide sufficient time to develop a plan to comply with the provisions of this act.

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, that other legal entity. For these purposes, "control" or "controlled" means ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 6 (1) through (4) of this act is being made by the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(3) "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.

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

(5) "Consent" means a clear affirmative act signifying a freely given, 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, including by electronic means, 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) "Decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

(10) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be associated with a natural person; (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and (c) contractually obligates any recipients of the information to comply with all provisions of this subsection.

(11) "Enroll," "enrolled," or "enrolling" means the process by which a facial recognition service creates a facial template from one or more images of a consumer and adds the facial template to a gallery used by the facial recognition service for identification, verification, or persistent tracking of consumers. It also includes the act of adding an existing facial template directly into a gallery used by a facial recognition service.

(12) "Facial recognition service" means technology that analyzes facial features and is used for the identification, verification, or persistent tracking of consumers in still or video images.

(13) "Facial template" means the machine-interpretable pattern of facial features that is extracted from one or more images of a consumer by a facial recognition service.

(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) "Identification" means the use of a facial recognition service by a controller to determine whether an unknown consumer matches any consumer whose identity is known to the controller and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

(18) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

(19) "Institutions of higher education" has the same meaning as in RCW 28B.92.030.

(20) "Local government" has the same meaning as in RCW 39.46.020.

(21) "Meaningful human review" means review or oversight by one or more individuals who are trained in accordance with section 17(9) of this act and who have the authority to alter the decision under review.

(22) "Nonprofit corporation" has the same meaning as in RCW 24.03.005.

(23) "Ongoing surveillance" means tracking the physical movements of a specified individual through one or more public places over time, whether in real time or through application of a facial recognition service to historical records. It does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time after the individual has been recognized.

(24) "Persistent tracking" means the use of a facial recognition service to track the movements of a consumer on a persistent basis without identification or verification of that consumer. Such tracking becomes persistent as soon as:

(a) The facial template that permits the tracking uses a facial recognition service for more than forty-eight hours after the first enrolling of that template; or

(b) The data created by the facial recognition service in connection with the tracking of the movements of the consumer are linked to any other data such that the consumer who has been tracked is identified or identifiable.

(25)(a) "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 or publicly available information.

(b) For purposes of this subsection, "publicly available information" means information that is lawfully made available from federal, state, or local government records.

(26) "Process" or "processing" means any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(27) "Processor" means a natural or legal person who processes personal data on behalf of a controller.

(28) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(29) "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.

(30) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(31) "Recognition" means the use of a facial recognition service to determine whether:

(a) An unknown consumer matches any consumer who has been enrolled in a gallery used by the facial recognition service; or

(b) An unknown consumer matches a specific consumer who has been enrolled in a gallery used by the facial recognition service.

(32)(a) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

(b) "Sale" does not include the following: (i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of information that the consumer

(A) intentionally made available to the general public via a channel of mass media, and (B) did not restrict to a specific audience; or (v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(33) "Security or safety purpose" means physical security, protection of consumer data, safety, fraud prevention, or asset protection.

(34) "Sensitive data" means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (c) the personal data from a known child; or (d) specific geolocation data. "Sensitive data" is a form of personal data.

(35) "Serious criminal offense" means any felony under chapter 9.94A RCW or an offense enumerated by Title 18 U.S.C. Sec. 2516.

(36) "Specific geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with the precision and accuracy below one thousand seven hundred fifty feet. Specific geolocation data excludes the content of communications.

(37) "State agency" has the same meaning as in RCW 43.105.020.

(38) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated web sites or online applications to predict such consumer's preferences or interests. It does not include advertising: (a) Based on activities within a controller's own web sites or online applications; (b) based on the context of a consumer's current search query or visit to a web site or online application; or (c) to a consumer in response to the consumer's request for information or feedback.

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

(40) "Verification" means the use of a facial recognition service by a controller to determine whether a consumer is a specific consumer whose identity is known to the controller and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

NEW SECTION. **Sec. 4.** JURISDICTIONAL SCOPE. (1) This chapter applies to legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) During a calendar year, controls or processes personal data of one hundred thousand consumers or more; or

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

(2) This chapter does not apply to:

(a) State agencies, local governments, or tribes;

(b) Municipal corporations;

(c) Information that meets the definition of:

(i) Protected health information for purposes of the federal health insurance portability and accountability act of 1996 and related regulations;

(ii) Health care information for purposes of chapter 70.02 RCW;

(iii) Patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

(iv) Identifiable private information for purposes of the federal policy for the protection of human subjects, 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation; the protection of human subjects under 21 C.F.R. Parts 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this subsection;

(v) Information and documents created specifically for, and collected and maintained by:

(A) A quality improvement committee for purposes of RCW 43.70.510, 70.230.080, or 70.41.200;

(B) A peer review committee for purposes of RCW 4.24.250;

(C) A quality assurance committee for purposes of RCW 74.42.640 or 18.20.390;

(D) A hospital, as defined in RCW 43.70.056, for reporting of health care-associated infections for purposes of RCW 43.70.056, a notification of an incident for purposes of RCW 70.56.040(5), or reports regarding adverse events for purposes of RCW 70.56.020(2)(b);

(vi) Information and documents created for purposes of the federal health care quality improvement act of 1986, and related regulations;

(vii) Patient safety work product for purposes of 42 C.F.R. Part 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

(viii) Information that is (A) deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164, and (B) derived from any of the health care-related information listed in this subsection (2)(c);

(d) Information originating from, and intermingled to be indistinguishable with, information under (c) of this subsection that is maintained by:

(i) A covered entity or business associate as defined by the health insurance portability and accountability act of 1996 and related regulations;

(ii) A health care facility or health care provider as defined in RCW 70.02.010; or

(iii) A program or a qualified service organization as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

(e) Information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512;

(f)(i) An activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.

(ii) (f)(i) of this subsection shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the fair credit reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the fair credit reporting act;

(g) Personal data collected and maintained for purposes of chapter 43.71 RCW;

(h) Personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

(i) Personal data collected, processed, sold, or disclosed pursuant to the federal driver's privacy protection act of 1994 (18 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or disclosure is in compliance with that law;

(j) Personal data regulated by the federal family educations rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing regulations;

(k) Personal data regulated by the student user privacy in education rights act, chapter 28A.604 RCW;

(l) Personal data collected, processed, sold, or disclosed pursuant to the federal farm credit act of 1971 (as amended in 12 U.S.C. Sec. 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et seq.) if the collection, processing, sale, or disclosure is in compliance with that law; or

(m) Data maintained for employment records purposes.

(3) Controllers that are in compliance with the verifiable parental consent mechanisms under the children's online privacy protection act, Title 15 U.S.C. Sec. 6501 through 6506 and its implementing regulations, shall be deemed compliant with any obligation to obtain parental consent under this chapter.

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

(2) Processors are responsible under this chapter for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. Such assistance shall include the following:

(a) Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6 of this act; and

(b) Taking into account the nature of processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to RCW 19.255.010; and shall provide information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 9 of this act.

(3) Notwithstanding the instructions of the controller, a processor shall:

(a) Implement and maintain reasonable security procedures and practices to protect personal data, taking into account the context in which the personal data are to be processed;

(b) Ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

(c) Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(4) Processing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties. In addition, the contract shall include the requirements imposed by this subsection and subsection (3) of this section, as well as the following requirements:

(a) At the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(b)(i) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and (ii) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor; alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and audit procedure for such audits as applicable, and shall provide a report of such audit to the controller upon request.

(5) In no event shall any contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this chapter.

(6) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to such processing.

NEW SECTION. **Sec. 6.** CONSUMER PERSONAL DATA RIGHTS. Consumers may exercise the rights set forth in this section by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise. In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise the rights of this chapter on the child's behalf. Except as provided in this chapter, the controller must comply with a request to exercise the rights pursuant to subsections (1) through (5) of this section.

(1) *Right of access.* A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access such personal data.

(2) *Right to correction.* A consumer has the right to correct inaccurate personal data concerning the consumer, taking into account

the nature of the personal data and the purposes of the processing of the personal data.

(3) *Right to deletion.* A consumer has the right to delete personal data concerning the consumer.

(4) *Right to data portability.* A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(5) *Right to opt out.* A consumer has the right to opt out of the processing of personal data concerning such consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

(6) *Responding to consumer requests.* (a) A controller must inform a consumer of any action taken on a request under subsections (1) through (5) of this section without undue delay and in any event within forty-five days of receipt of the request. That period may be extended once by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within forty-five days of receipt of the request, together with the reasons for the delay.

(b) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within forty-five days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subsection (7) of this section.

(c) Information provided under this section must be provided by the controller free of charge, up to twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) Charge a reasonable fee to cover the administrative costs of complying with the request, or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(d) A controller is not required to comply with a request to exercise any of the rights under subsections (1) through (4) of this section if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to authenticate the request.

(7)(a) Controllers must establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights under subsections (1) through (5) of this section within a reasonable period of time after the consumer's receipt of the notice sent by the controller under subsection (6)(b) of this section.

(b) The appeal process must be conspicuously available and as easy to use as the process for submitting such requests under this section.

(c) Within thirty days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by sixty additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any such extension within thirty days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to (c) of this subsection, the controller must clearly and prominently ask the consumer whether the consumer consents to having the controller submit the appeal, along with any action taken or not taken by the controller in response to the appeal and must, upon request, provide the controller's written explanation of the reasons in support thereof, to the attorney general. If the consumer provides such consent, the controller must submit such information to the attorney general.

NEW SECTION. **Sec. 7.** PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA. (1) This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:

(a) Reidentify deidentified data;

(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data pursuant to section 6 (1) through (4) of this act, if all of the following are true:

(i)(A) The controller is not reasonably capable of associating the request with the personal data, or (B) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(iii) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section; or

(c) Maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(2) The rights contained in section 6 (1) through (4) of this act do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(3) A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject, and must take appropriate steps to address any breaches of contractual commitments.

NEW SECTION. **Sec. 8.** RESPONSIBILITIES OF CONTROLLERS. (1) *Transparency.*

(a) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(i) The categories of personal data processed by the controller;

(ii) The purposes for which the categories of personal data are processed;

(iii) How and where consumers may exercise the rights contained in section 6 of this act, including how a consumer may appeal a controller's action with regard to the consumer's request;

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

(v) The categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells personal data to third parties or processes personal data for targeted advertising, it must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing, in a clear and conspicuous manner.

(c) Controllers shall establish, and shall describe in the privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their rights under this chapter. Such means shall take into account the ways in which consumers interact with the controller, the need for secure and reliable communication of such requests, and the controller's ability to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this chapter.

(2) *Purpose specification.* A controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.

(3) *Data minimization.* A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.

(4) *Avoid secondary use.* Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(5) *Security.* A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

(6) *Nondiscrimination.* A controller may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection shall not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. A controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose. A controller may not enroll a consumer in a facial recognition service in connection with a bona fide loyalty, rewards, premium features, discounts, or club card program.

(7) *Sensitive data.* Except as otherwise provided in this act, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the children's online privacy protection act requirements.

(8) *Nonwaiver of consumer rights.* Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable.

NEW SECTION. **Sec. 9.** DATA PROTECTION ASSESSMENTS. (1) Controllers must conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising;

(b) The sale of personal data;

(c) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

(d) The processing of sensitive data; and

(e) Any processing activities involving personal data that present a heightened risk of harm to consumers.

Such data protection assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the personal data are to be processed.

(2) Data protection assessments conducted under subsection (1) of this section must 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. 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, must be factored into this assessment by the controller.

(3) The attorney general may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data protection assessments for compliance with the responsibilities contained in section 8 of this act and with other laws including, but not limited to, chapter 19.86 RCW. Data protection assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection

does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(4) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under this section if they have a similar scope and effect.

NEW SECTION. **Sec. 10.** LIMITATIONS AND APPLICABILITY. (1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

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

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

(c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(d) Investigate, establish, exercise, prepare for, or defend legal claims;

(e) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(f) Take immediate steps to protect an interest that is essential for the life of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(g) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(h) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws if the deletion of the information is likely to render impossible or seriously impair the achievement of the research and the consumer provided consent; or

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

(2) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data to:

(a) Conduct internal research solely to improve or repair products, services, or technology;

(b) Identify and repair technical errors that impair existing or intended functionality; or

(c) Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(3) 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.

(4) 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 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 in compliance with the requirements of this chapter is likewise not in violation of this chapter for the obligations of the controller or processor from which it receives such personal data.

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

(a) Adversely affect the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution; or

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

(6) Personal data that are processed by a controller pursuant to this section must not be processed for any purpose other than those

expressly listed in this section. Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such processing is: (i) Necessary, reasonable, and proportionate to the purposes listed in this section; and (ii) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section. Furthermore, personal data that are collected, used, or retained pursuant to subsection (2) of this section must, insofar as possible, taking into account the nature and purpose or purposes of such collection, use, or retention, be subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (6) of this section.

(8) Processing personal data solely for the purposes expressly identified in subsection (1)(a) through (d) or (g) of this section does not, by itself, make an entity a controller with respect to such processing.

NEW SECTION. **Sec. 11.** LIABILITY. (1) Any violation of this chapter shall not serve as the basis for, or be subject to, a private right of action under this chapter or under any other law. This does not relieve any party from any duties or obligations imposed, or to alter any independent rights that consumers have under other laws, chapter 19.86 RCW, the Washington state Constitution, or the United States Constitution.

(2) 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.

NEW SECTION. **Sec. 12.** ENFORCEMENT. (1) The attorney general has exclusive authority to enforce this chapter by bringing an action in the name of the state, or as parens patriae on behalf of persons residing in the state.

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

NEW SECTION. **Sec. 13.** CONSUMER PRIVACY ACCOUNT. The consumer privacy account is created in the state treasury. All receipts from the imposition of civil penalties under this chapter must be deposited into the account except for the recovery of costs and attorneys' fees accrued by the attorney general in enforcing this chapter. Moneys in the account may be spent only after appropriation. Moneys in the account may only be used for the purposes of the office of privacy and data protection as created under RCW 43.105.369, and may not be used to supplant general fund appropriations to the agency.

NEW SECTION. **Sec. 14.** 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. 15.** ATTORNEY GENERAL REPORT. (1) The attorney general shall compile a report evaluating the liability and enforcement provisions of this chapter including, but not limited to, the effectiveness of its efforts to enforce this chapter, and any recommendations for changes to such provisions.

(2) The attorney general shall submit the report to the governor and the appropriate committees of the legislature by July 1, 2022.

NEW SECTION. **Sec. 16.** JOINT RESEARCH INITIATIVES. The governor may enter into agreements with the governments of the Canadian province of British Columbia and the states of California and Oregon for the purpose of sharing personal data or personal information by public bodies across national and state borders to enable collaboration for joint data-driven research initiatives. Such agreements must provide reciprocal protections that the respective governments agree appropriately safeguard the data.

NEW SECTION. **Sec. 17.** FACIAL RECOGNITION. (1) Processors that provide facial recognition services must make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations: PROVIDED, That making such an application programming interface or other technical capability available does not require the disclosure of proprietary data, trade secrets, intellectual property, or other information, or if doing so would increase the risk of cyberattacks including, without limitation, cyberattacks related to unique methods of conducting business, data unique to the product or services, or determining prices or rates to be charged for services. Such subpopulations are defined by visually detectable characteristics, such as (a) race, skin tone, ethnicity, gender, age, or disability status, or (b) other protected characteristics that are objectively determinable or self-identified by the individuals portrayed in the testing dataset. If the results of that independent testing identify material unfair performance differences across subpopulations and the methodology, data, and results are disclosed in a manner that allow full reproduction of the testing directly to the processor, who, acting reasonably, determines that the methodology and results of that testing are valid, then the processor must develop and implement a plan to mitigate the identified performance differences. Nothing in this subsection prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.

(2) Processors that provide facial recognition services must provide documentation that includes general information that:

(a) Explains the capabilities and limitations of the services in plain language; and

(b) Enables testing of the services in accordance with this section.

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

(4) Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public that includes, at minimum, the following:

(a) The purpose or purposes for which the facial recognition service is deployed; and

(b) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to, a link to any applicable online notice, terms, or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.

(5) Controllers must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premise open to the public.

(6) As an exception to subsection (5) of this section, controllers may enroll an image of a consumer in a facial recognition service for a security or safety purpose without first obtaining consent from that consumer, provided that all of the following requirements are met:

(a) The controller must hold a reasonable suspicion, based on a specific incident, that the consumer has engaged in criminal activity, which includes, but is not limited to, shoplifting, fraud, stalking, or domestic violence;

(b) Any database used by a facial recognition service for identification, verification, or persistent tracking of consumers for a security or safety purpose must be used solely for that purpose and maintained separately from any other databases maintained by the controller;

(c) The controller must review any such database used by the controller's facial recognition service no less than annually to remove facial templates of consumers whom the controller no longer holds a reasonable suspicion that they have engaged in criminal activity; and

(d) The controller must establish an internal process whereby a consumer may correct or challenge the decision to enroll the image of the consumer in a facial recognition service for a security or safety purpose.

(7) Controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.

(8) Prior to deploying a facial recognition service in the context in which it will be used, controllers using a facial

recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must test the facial recognition service in operational conditions. Controllers must take commercially reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the facial recognition service.

(9) Controllers using a facial recognition service must conduct periodic training of all individuals that operate a facial recognition service or that process personal data obtained from the use of facial recognition services. Such training shall include, but not be limited to, coverage of:

(a) The capabilities and limitations of the facial recognition service;

(b) Procedures to interpret and act on the output of the facial recognition service; and

(c) The meaningful human review requirement for decisions that produce legal effects on consumers or similarly significant effects on consumers, to the extent applicable to the deployment context.

(10) Controllers shall not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency, except when such disclosure is:

(a) Pursuant to the consent of the consumer to whom the personal data relates;

(b) Required by federal, state, or local law in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury;

(c) Necessary to prevent or respond to an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the controller; or

(d) To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec. 2258A.

(11) Controllers that deploy a facial recognition service must respond to a consumer request to exercise the rights specified in section 6 of this act and must fulfill the responsibilities identified in section 8 of this act.

(12) Voluntary facial recognition services used to verify an aviation passenger's identity in connection with services regulated by the secretary of transportation under Title 49 U.S.C. Sec. 41712 and exempt from state regulation under Title 49 U.S.C. Sec.

41713(b)(1) are exempt from this section. Images captured by an airline must not be retained for more than twenty-four hours and, upon request of the attorney general, airlines must certify that they do not retain the image for more than twenty-four hours. An airline facial recognition service must disclose and obtain consent from the customer prior to capturing an image.

NEW SECTION. **Sec. 18.** This chapter does not apply to institutions of higher education or nonprofit corporations until July 31, 2024.

NEW SECTION. **Sec. 19.** Sections 1 through 18 and 20 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 20.** This act takes effect July 31, 2021.

--- END ---