S-1373.7

SUBSTITUTE SENATE BILL 5376

State of Washington 66th Legislature 2019 Regular Session

By Senate Environment, Energy & Technology (originally sponsored by Senators Carlyle, Palumbo, Wellman, Mullet, Pedersen, Billig, Hunt, Liias, Rolfes, Saldaña, Hasegawa, and Keiser)

READ FIRST TIME 02/18/19.

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) Washingtonians cherish privacy as an element of their individual freedom.

(b) Washington is a technology leader on a national and global level and recognizes its distinctive position in promoting the efficient balance of consumer privacy and economic benefits.

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

(d) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. This growth has the potential for great benefits to human knowledge,

technological innovation, and economic growth, but also the potential to harm individual privacy and freedom.

(e) Millions of Washingtonians have been affected by electronic data breaches and the resulting loss of privacy, and the net effect, both financially and in the chilling of consumer confidence, has and will continue to cost Washington state businesses.

(f) As technology and businesses continue to push the limits of data collection with exponential rapidity, laws must keep pace as technology and business practices evolve to protect businesses and consumers.

(g) There is a need to preserve individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information. Meeting this need will promote continued innovation and economic growth in the networked economy.

(h) Enforcement of general principles in law will ensure that citizens continue to enjoy meaningful privacy protections while affording ample flexibility for technologies and business models to evolve.

(i) The European Union recently updated its privacy law through the passage and implementation of the general data protection regulation, affording its residents the strongest privacy protections in the world. Washington residents deserve to enjoy the same level of robust privacy safeguards.

(j) In addition, the technology industry has been a tremendous driver of economic growth in Washington state. We need to ensure that any new privacy laws not only provide Washington residents with strong privacy protections but also enable industry and others to use data to create innovative technologies, products, and solutions.

(k) Technology will continue to evolve and change. Consequently, any new privacy laws must be technology neutral and flexible, so that they may apply not only to the technologies and products of today, but to the technologies and products of tomorrow.

(l) Washington residents have long enjoyed an expectation of privacy in their public movements. The development of new technology like facial recognition could, if deployed indiscriminately and without guardrails, enable the constant surveillance of any individual any time of the day and every day of the year. Washington residents should have the right to a reasonable expectation of privacy in their movements, and thus should be free from ubiquitous

and surreptitious surveillance using facial recognition technology. Further, Washington residents should have the right to expect information about the capabilities and limitations of facial recognition technology and that it should not be deployed by private sector organizations without proper public notice.

(2) As such, the legislature recognizes the consumer protection principles in this act regarding transparency, individual control, respect for context, focused collection and responsible use, security, access, and accuracy.

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) The phrase "sells or licenses" does not include:

(i) A one-time or occasional sale of assets that is not part of the ordinary conduct of the business;

(ii) A sale or license of data that is merely incidental to the business; or

(iii) 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.

(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 by a third party, other than the original controller or processor, for advertising purposes or to market goods.

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

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

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

(16) "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.

(17) "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. For these purposes, "publicly available information" means information that is lawfully made available from federal, state, or local government records.

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

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

(20) "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.

(21) "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.

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

(23)(a) "Sale," "sell," or "sold" means the exchange of personal data for monetary 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.

(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 or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) 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.

(24) "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.

(25) "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. It does not include advertising to a consumer based upon the consumer's current visit to a web site, application, or online service, or in response to the consumer's request for information or feedback.

(26) "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.

(27) "Verified 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 commercially reasonable means.

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 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 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 and local governments;

(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. 290 dd-2;

(iv) Identifiable private information for purposes of the federal policy for the protection of human subjects, 45 C.F.R. Part 46, or 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, or the protection of human subjects under 21 C.F.R. Parts 50 and 56;

(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 specifically for the federal health care quality improvement act of 1986, and related regulations; or

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

(d) Information maintained in the same purposes as information under (c) of this subsection 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. 290 dd-2;

(e) The sale of personal data to or from a consumer reporting agency if that data is reported in, or used to generate, a consumer report as defined by 15 U.S.C. Sec. 1681a(d), and use of that data is limited by the federal fair credit reporting act (15 U.S.C. Sec. 1681 et seq.);

(f) 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;

(g) 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; or

(h) Data maintained for employment records purposes.

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. Controllers shall facilitate verified requests to exercise the consumer rights set forth in subsections (1) through (6) of this section.

(1) Upon a verified request from a consumer, a controller must confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data that the controller maintains in identifiable form concerning the consumer.

(a) Upon a verified request from a consumer, a controller must provide a copy of the personal data that the controller maintains in identifiable form undergoing processing. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information must be provided in a commonly used electronic form.

(b) This subsection does not adversely affect the rights or freedoms of others.

(2) Upon a verified request from a consumer, the controller, without undue delay, must correct inaccurate personal data that the controller maintains in identifiable form concerning the consumer. Taking into account the business purposes of the processing, the controller must complete incomplete personal data, including by means of providing a supplementary statement where appropriate.

(3)(a) Upon a verified request from a consumer, a controller must delete, without undue delay, the consumer's personal data that the controller maintains in identifiable form if one of the following grounds applies:

(i) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer;

(ii) For processing that requires consent under section 8(3) of this act, the consumer withdraws consent to processing and there are no business purposes for the processing;

(iii) The consumer objects to the processing pursuant to subsection (6) of this section and (A) there are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public, for which the processing is necessary; or (B) the processing is for direct marketing purposes;

(iv) The personal data has been unlawfully processed; or

(v) The personal data must be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject.

(b) Where the controller is obliged to delete personal data that the controller maintains in identifiable form under this section that has been disclosed to third parties by the controller, including data brokers that received the personal data through a sale, the controller must take reasonable steps, which may include technical measures, to inform other controllers of which it is aware that are processing such personal data, and that received such personal data from the controller or are processing such personal data on behalf of the controller, that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must take into account available technology and cost of implementation.

(c) This subsection does not apply to the extent processing is necessary:

(i) For exercising the right of free speech;

(ii) For compliance with a legal obligation that requires processing of personal data by federal, state, or local law, regulation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) For reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(iv) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the

deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;

(v) For the establishment, exercise, or defense of legal claims; or

(vi) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity.

(4)(a) Upon a verified request from a consumer, the controller must restrict processing of personal data that the controller maintains in identifiable form if the purpose for which the personal data is (i) not consistent with a purpose for which the personal data was collected; (ii) not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or (iii) unlawful.

(b) Where personal data is subject to a restriction of processing under this subsection, the personal data must, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; (iii) for the protection of the rights of another natural or legal person; (iv) for reasons of important public interest under federal, state, or local law; (v) to provide products or services requested by the consumer; or (vi) for another purpose set forth in subsection (3)(c) of this section.

(c) A consumer who has obtained restriction of processing pursuant to this subsection must be informed by the controller before the restriction of processing is lifted.

(5)(a) Upon a verified request from a consumer, the controller must provide to the consumer, if technically feasible and commercially reasonable, any personal data that the controller maintains in identifiable form concerning the consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section 8(3) of this act, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.

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

(c) The rights provided in this subsection do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not adversely affect the rights of others.

(6)(a) A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of personal data concerning such consumer.

(b) When a consumer objects to the processing of their personal data for direct marketing purposes, which includes the sale of personal data concerning the consumer to third parties for direct marketing purposes and targeted advertising, the controller must no longer process the personal data subject to the objection for such purpose and must take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third parties to whom the controller sold the consumer's personal data for such purposes. Third parties must honor objection requests pursuant to this subsection received from third-party controllers.

(c) If a consumer objects to processing for any purposes, other than direct marketing, the controller may continue processing the personal data subject to the objection if the controller can demonstrate a compelling business purpose to process such personal data, or if another exemption in this chapter applies.

(7) A controller must communicate any correction, deletion, or restriction of processing carried out in accordance with subsections (2), (3), or (4) of this section to each third-party recipient to whom the controller knows the personal data has been disclosed, including third parties that received the data through a sale, within one year preceding the verified request unless this proves functionally impractical, technically infeasible, or involves disproportionate effort. The controller must inform the consumer about such third-party recipients or categories, if any, if the consumer requests such information.

(8) A controller must provide information on action taken on a verified request under subsections (1) through (6) of this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty 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 thirty days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information must be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) 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 thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) 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, in particular because of their repetitive character, the controller may either: (i) Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subsections (1) through (6) of this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

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; and

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

(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.** RISK ASSESSMENTS. (1) Controllers must conduct, to the extent not previously conducted, 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. Such risk assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is to be processed.

(2) Risk 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 factor into this assessment by the controller.

(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 or if another exemption under this chapter applies. To the extent the controller seeks consumer consent for processing, such consent shall be as easy to withdraw as to give.

(4) Processing for a business purpose shall be presumed to be permissible unless: (a) It involves the processing of sensitive data; and (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

(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. 9.** 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. 10.** EXEMPTIONS. (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 law;

(d) Investigate, exercise, or defend legal claims;

(e) Prevent or detect identity theft, fraud, or other criminal activity or verify identities;

(f) 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;

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

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

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

(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 11 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 11 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 (1) through (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. 11.** LIABILITY. (1) This chapter does not serve as the basis for a private right of action under this chapter or any other law.

(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 shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

NEW SECTION. **Sec. 12.** 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) A controller or processor is in violation of this chapter if it fails to cure any alleged violation of sections 6 through 10 of this act within thirty days after receiving notice of alleged noncompliance. 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.

(4) 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. 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.

NEW SECTION. **Sec. 13.** 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. 14.** FACIAL RECOGNITION. (1) Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects concerning consumers or similarly significant effects concerning consumers. Decisions producing legal effects or similarly significant effects shall include, but not be limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(2) 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.

(3) 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.

(4) 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 constitute a consumer's consent to the use of such facial recognition services when that consumer enters those premises that have such notice.

(5) 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.

(6) For purposes of this section, "facial recognition" means technology that analyzes facial features and is used for the unique personal identification of natural persons in still or video images.

NEW SECTION. **Sec. 15.** A new section is added to chapter 9.73 RCW to read as follows:

(1) State and local government agencies shall not use facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces, unless such use is in support of law enforcement activities and either (a) a court order has been obtained to permit the use of facial recognition services for that ongoing surveillance; or (b) where there is an emergency involving imminent danger or risk of death or serious physical injury to a person.

(2) This section applies to all Washington state and local government agencies.

(3) For purposes of this section, "facial recognition" means the same as in section 14 of this act.

Sec. 16. 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, 2023, 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. 17.** Sections 3 through 14 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 18.** This act takes effect July 30, 2021.

--- END ---