2SSB 5376 - H COMM AMD
By Committee on Innovation, Technology & Economic Development

NOT CONSIDERED 12/23/2019

Strike everything after the enacting clause and insert the following:

"NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and cited as the Washington privacy act of 2019.

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

(a) Washington explicitly recognizes its people's right to privacy under Article I, section 7 of the state Constitution. Nothing in this act diminishes this right.

(b) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. The protection of individual privacy and freedom in relation to the processing of personal data requires the recognition of the principle that consumers retain ownership interest of their personal data, including personal data that undergoes processing or is in possession of another party. Consumers desire greater transparency and control over the collection, disclosure, and sharing of their personal data.

(c) Nothing in this act affects the consumer protections in chapter 19.86 RCW, the consumer protection act.

(d) Personal data should be collected with a clear purpose and with consumers' consent.

(2) Possession of personal data brings with it an obligation of care and to fulfill requirements under this act, no matter the source of data, or the size of the entity holding or processing personal data. To preserve trust and confidence that personal data will be protected appropriately, the legislature recognizes that with regard to processing of personal data, Washington consumers have the rights to:

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

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

(c) Correct inaccurate personal data;

(d) Obtain deletion of personal data;

(e) Restrict processing of personal data;

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

(g) Object to processing of personal data; and

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

(3) 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.

(4) 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 proper regulation, enable the constant surveillance of any individual. 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 have the right to information about the capabilities, possible bias, and limitations of facial recognition technology and that it should not be deployed by private sector organizations without proper public notice.

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 purpose" means the processing of a consumer's personal data with the consumer's consent for the controller's or its processor's operational 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) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, prosecuting those responsible for that activity, and notifying consumers of illegal activity that impacts personal data;

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

(c) 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;

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

(e) Undertaking internal research for technological development, if conducted with deidentified data; or

(f) Authenticating a consumer's identity at the request of the consumer or for compliance with this act.

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

(4) "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 or other clear affirmative action.

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

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

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

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

(c) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of

or as a function of a telecommunications carrier, does not qualify the business as a data broker.

(8) "Deidentified data" means data from which direct and known indirect identifiers have been removed or manipulated to break the linkage to a known natural person and to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prohibit or to prevent reidentification may include legal, administrative, technical, or contractual controls.

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

(10) "Direct identifier" means data that identifies a natural person directly without additional information or by linking to publicly available information. "Direct identifier" includes, but is not limited to, name, address, biometric data, social security number, or any government-issued identification number.

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

(12) "Facial recognition" means technology that maps a person's unique facial features for purposes of identifying or verifying the person, or to discern the person's demographic information, such as gender, race, age, nationality, or sexual orientation, or emotional state or mood. "Facial recognition" includes facial verification, facial identification, and facial characterization, and generates facial recognition data that is subject to this act. "Facial recognition" does not include facial detection, whereby facial mapping is done solely for the purpose of distinguishing the presence from the absence of a human face without storing facial recognition data upon completion.

(13) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly, in particular by reference to an identifier, including, but not limited to, a name, an online identifier, an identification number, biometric data, or specific geolocation data.

(14) "Indirect identifier" means data that identifies a natural person indirectly or helps connect pieces of data until a natural person can be singled out. "Indirect identifier" includes, but is not limited to, gender, date of birth, or internet protocol address.

(15) "Legal effects" means, without limitation, denial of consequential services or support, such as financial and lending

services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and other similarly significant effects.

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

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

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

(19) "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.

(20) "Privacy harm" means harm that results when personal data is processed, shared, disclosed, or sold in unknown, unexpected, or impermissible ways. "Privacy harm" is not limited to harm that results in a provable monetary loss or other tangible harm.

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

(22) "Restriction of processing" means the marking of stored personal data so that its processing is limited.

(23)(a) "Sale," "sell," or "sold" means the exchange or disclosure of personal data for consideration by the controller to another party. A sale must be consistent with consumer consent and the purposes for which the sold personal data was collected.

(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 contractual 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, if consumers are notified of the transfer of their data and of their rights under this chapter; 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, if consumers are notified of the transfer of their data and of their rights under this chapter.

(24) "Sensitive data" means (a) personal data revealing racial or ethnic origin, citizenship, immigration status, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation; (b) genetic or biometric data; or (c) the personal data of a known child.

(25) "Targeted advertising" means displaying to a consumer selected advertisements based on the consumer's personal data obtained or inferred over time from the consumer's activities across nonaffiliated web sites, applications, or online services to predict user preferences or interests. "Targeted advertising" does not include advertising to a consumer based upon the consumer's visits to a web site, application, or online service that a reasonable consumer would believe to be associated with the publisher where the ad is placed based on common branding, trademarks, or other indicia of common ownership, 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 verify the legitimacy of the request and identity of the consumer making the request using 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.

(2) This chapter does not apply to:

(a) State or local government;

(b) Municipal corporations; and

(c) Institutions of higher education, as defined in RCW 28B.10.016, and private, not-for-profit institutions of higher education.

(3) This chapter does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

(4) This chapter does not apply to the following information:

(a) Protected health information for purposes of the federal health insurance portability and accountability act of 1996, the federal health information technology for economic and clinical health act, and related regulations;

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

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

(d) 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 protection of human subjects under 21 C.F.R. Parts 50 and 56;

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

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

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

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

(iv) 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);

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

(g) 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;

(h) Information collected, used, or disclosed pursuant to chapter 43.71 RCW, if collection, use, or disclosure is in compliance with that law;

(i) Personal data provided to, from, or held by a consumer reporting agency as defined by 15 U.S.C. Sec. 1681a(f), but solely to the extent that such data is to be reported in, or used to generate, a consumer report, as defined by 15 U.S.C. Sec. 1681a(d), and only if the collection, processing, sale, or disclosure of such data is in compliance with the federal fair credit reporting act (15 U.S.C. Sec. 1681 et seq.);

(j) Personal data regulated by the children's online privacy protection act, 15 U.S.C. Secs. 6501 through 6506, if collected, processed, and maintained in compliance with that law;

(k) 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;

(l) 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

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

(n) Information about employees or employment status collected, processed, or used by an employer pursuant to and solely for the purposes of an employer-employee relationship.

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 chapter 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.

(4) Third parties are responsible for assisting controllers and processors in meeting their obligations under this chapter with regard to personal data third parties receive from controllers or processors. Third parties must comply with consumer requests made known to them by a controller.

(5) Controllers, processors, and third parties must adhere to the consent of a consumer with regard to the consumer's personal data.

NEW SECTION. **Sec. 6.** CONSUMER RIGHTS. (1) A consumer retains ownership interest in the consumer's personal data processed by a controller, a processor, or a third party and may exercise any of the consumer rights set forth in section 2 of this act by submitting to a controller a verified request that specifies which rights the consumer wishes to exercise. Controllers may not require consumers to create an account in order to make a verified request.

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

(3) Upon receiving a verified request from a consumer, a controller must:

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

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

(c) Provide in a commonly used electronic format a copy of the consumer's personal data that is undergoing processing;

(d) Provide in a structured, commonly used, and machine-readable format a copy of the consumer's personal data that the consumer has provided to the controller if the processing of the consumer's personal data:

(i)(A) Requires consent under section 9(3) of this act;

(B) Is necessary for the performance of a contract to which the consumer is a party; or

(C) Is done in order to take steps at the request of the consumer prior to entering into a contract; and

(ii) Is carried out by automated means;

(e) Correct the consumer's inaccurate personal data, or complete the consumer's incomplete personal data, including by means of providing a supplementary statement where appropriate;

(f) Delete the consumer's personal data, if one of the following grounds applies:

(i) The personal data is no longer necessary in relation to the purposes for which it was collected or processed;

(ii) The consumer withdraws consent for processing that requires consent under section 9(3) of this act, and there are no business purposes for processing;

(iii) Processing is for direct marketing or targeted advertising purposes;

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

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

(g) Take reasonable steps to inform other controllers or processors of which the controller is aware, and which are processing the consumer's personal data they received from the controller, that the consumer has requested deletion of any copies of or links to the consumer's personal data. Controllers and processors that receive notification of the consumer's deletion request must comply with that request;

(h) Restrict processing of the consumer's personal data if the purpose for which the personal data is being processed is inconsistent with a purpose for which the personal data was collected, inconsistent with a purpose disclosed to the consumer at the time of collection or authorization, or inconsistent with exercising the right of free speech. Where personal data is subject to a restriction of processing under this subsection, with the exception of storage, the personal data may only be processed with the consumer's consent or for purposes set forth in section 11 of this act, in which case the controller may not sell or otherwise disclose any personal data being processed pursuant to the claimed purposes. A controller must inform and gain consent from the consumer before any restriction of processing is lifted;

(i) Stop processing personal data of the consumer who objects to such processing, including the selling of the consumer's personal data to third parties for purposes of direct marketing or targeted advertising, without regard to the source of data. The controller must take reasonable steps to communicate a consumer's objection to processing to third parties to whom the controller sold the

consumer's personal data. Third parties must comply with the consumer's request made known to them by the controller;

(j) Take reasonable steps to communicate a consumer's objection to processing to third parties to whom the controller disclosed, including through sale, the consumer's personal data and who must comply with objection requests communicated by the controller.

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

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

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

(ii) The reasons for not taking action on the consumer's request, including a statement regarding any exemptions under section 11 of this act, and information about the process for internal review of the decision by the controller.

(5) A controller must communicate any correction, deletion, or restriction of processing carried out pursuant to a verified consumer request to each third party to whom the controller knows the consumer's personal data has been disclosed within one year preceding the verified request, including third parties that received the data through a sale. Third parties must comply with the consumer's requests made known to them by the controller.

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

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

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

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

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

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

(b) The categories of personal data that the controller shares with third parties;

(c) The purposes for which the categories of personal data are used by the controller and disclosed to third parties, if any;

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

(e) Information about the rights guaranteed to the consumers in section 2 of this act;

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

(g) A statement that the controller processes personal data of a consumer only pursuant to the consumer's consent and solely for the purposes disclosed to the consumer under this section.

(2) If a controller sells personal data to data brokers, it must disclose such sales, and the manner in which a consumer may object to such sales, in a clear and conspicuous manner.

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

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

(3) Controllers may report metrics on their public web site to demonstrate and corroborate their compliance with this chapter.

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

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

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

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

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

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

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

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

(4) Processing personal data for a business purpose must be described in the risk assessment, but is presumed permissible unless: (a) It involves the processing of sensitive data; (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards; (c) consent was not given; or (d) processing is inconsistent with consent given.

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

NEW SECTION. **Sec. 10.** DEIDENTIFIED DATA. A controller or processor that uses, sells, or shares deidentified data shall:

(1) Make a public commitment to not reidentify deidentified data;

(2) Provide by contract that third parties must not reidentify deidentified data received from a controller or a processor;

(3) Exercise reasonable oversight to monitor compliance with any contractual commitments to which deidentified data is subject; and

(4) Take appropriate steps to address any breaches of contractual commitments to which deidentified data is subject.

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

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

(d) Temporarily prevent, detect, or respond to security incidents;

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

(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) Process personal data of a consumer for one or more specific purposes where the consumer has given and not withdrawn their consent to the processing for those purposes; or

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

(2) The office of privacy and data protection created in RCW 43.105.369 may grant controllers one-year waivers to permit processing that is necessary:

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

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

(c) To safeguard intellectual property rights; or

(d) To protect the vital interests of the consumer or of another natural person.

(3) A controller may not sell any personal data processed under subsections (1) and (2) of this section.

(4) 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.

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

(a) Reidentify deidentified data; or

(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.

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

(2) Controllers shall not use facial recognition for profiling or to make decisions that produce legal effects concerning consumers including, but not limited to, denial of consequential service or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

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

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

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

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

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

(8) Nothing in this section restricts a controller's or processor's ability to prevent, detect, or respond to security incidents, or to protect against theft, fraud, or other malicious or deceptive activities.

NEW SECTION. **Sec. 13.** LIABILITY. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability must be allocated among the parties according to principles of comparative fault, unless liability is otherwise allocated by contract among the parties.

NEW SECTION. **Sec. 14.** ENFORCEMENT. 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.

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

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

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

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

(a) To conduct an annual privacy review;

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

(c) To articulate privacy principles and best practices;

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

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

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

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

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

(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been

achieved. These performance measures must include, but are not limited to, the following:

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

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

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

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

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

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

(8) The office of privacy and data protection must conduct an analysis on the public and private sector use of facial recognition. By September 30, 2020, the office of privacy and data protection must submit a report of its findings and recommendations for use or limits to use of facial recognition technology to the appropriate committees of the legislature.

(9) The office of privacy and data protection must conduct a study on whether the federal health insurance portability and accountability act of 1996, the federal health information technology

for economic and clinical health act, and related regulations adequately protect personal health information and prevent it from being bought, sold, or traded on a commercial basis. By December 31, 2020, the office of privacy and data protection must submit a report of its findings to the appropriate committees of the legislature.

(10) The office of privacy and data protection must convene a work group to study the best practices for ensuring consumers understand their privacy rights prior to agreeing to terms of service, terms of agreement, and other similar documents. The work group should consider the efficacy of summaries, abstracts, and other explanatory measures. By July 31, 2021, the office of privacy and data protection must submit a report of its findings and recommendations to the appropriate committees of the legislature.

(11) The office of privacy and data protection, in consultation with the attorney general, must by rule clarify definitions of this chapter as necessary. The office of privacy and data protection may create rules for granting waivers for purposes of section 11(2) of this act.

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

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

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

(3) All use of facial recognition must be in compliance with Article I, section 7 of the state Constitution.

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

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

NEW SECTION. **Sec. 19.** This act is subject to appropriations in the omnibus appropriations act.

NEW SECTION. **Sec. 20.** If any provision of this act is found to be in conflict with federal or state law or regulations, the conflicting provision of this act is declared to be inoperative.

NEW SECTION. **Sec. 21.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 22.** This act takes effect July 30, 2020, except for section 15 which takes effect ninety days after final adjournment of the legislative session in which this act is enacted."

Correct the title.

EFFECT: (1) Sets forth the principle that consumers retain ownership interest in their personal data, including personal data that undergoes processing, and enumerates specific consumer rights with regard to processing of personal data.

(2) Provides that personal data should be collected with a clear purpose and with consumers' consent, and that possession of personal data brings with it obligations of care.

(3) Modifies several key definitions, including "business purpose", "consent", "sale", "deidentified data", "sensitive data", and "facial recognition".

(4) Eliminates several definitions not used in the bill, such as "covered entity" and "health care facility".

(5) Creates several new definitions, such as "privacy harm", "direct identifiers", and "indirect identifiers".

(6) Eliminates the thresholds that a legal entity must meet in order for the obligations set forth in the bill to apply to that legal entity.

(7) Exempts certain information subject to enumerated federal and state laws from the provisions of the bill.

(8) Exempts institutions of higher education, as defined in the state law related to colleges and universities, and private, not-for-profit institutions of higher education from the provisions of the bill.

(9) Specifies that third parties are responsible for assisting controllers and processors in meeting their obligations under the bill with regard to personal data third parties receive from controllers or processors.

(10) Requires controllers, processors, and third parties to adhere to the consent of a consumer with regard to the consumer's personal data.

(11) Provides that a consumer retains ownership interest in the consumer's personal data processed by a controller or a processor and may exercise any of the consumer rights by submitting to a controller a verified request that specifies which rights the consumer wishes to exercise.

(12) Allows a controller to request additional reasonable information necessary to confirm the identity of the consumer making a request.

(13) Removes the qualification that the right to know about processing of personal data and the right of access, correction, or deletion applies to personal data that a controller maintains in an identifiable form.

(14) Removes the requirement to take into account the business purposes of the processing when completing incomplete personal data.

(15) Modifies the grounds for requiring that a controller delete a consumer's personal data and eliminates the circumstances in which the right to deletion does not apply.

(16) Requires controllers and processors notified of a consumer's deletion request to comply with that request.

(17) Modifies the right to restrict processing of personal data by requiring that any personal data subject to restriction be processed only with the consumer's consent or if an exemption applies, and prohibits the controller processing data pursuant to the claimed exemption from selling or otherwise disclosing that data.

(18) Provides that a controller must stop processing personal data of the objecting consumer regardless of whether the processing is for targeted advertising or other purposes, and that third parties notified of the consumer's objection must comply with the consumer's request.

(19) Eliminates the provisions that allow controllers to consider whether communicating certain consumer requests to third parties is functionally impractical, technically infeasible, or involves disproportionate effort.

(20) Removes the authorization for controllers to charge a reasonable fee when complying with manifestly unfounded or repetitive consumer requests.

(21) Provides that a controller must make publicly available all policies adopted and used by the controller to comply with the provision related to consumer rights.

(22) Sets forth additional requirements for information that must be included in a controller's privacy notice, such as a statement that the controller processes personal data only pursuant to a consumer's consent and solely for the purposes disclosed to the consumer in the privacy notice.

(23) Requires controllers to develop, implement, and make publicly available an annual plan for complying with the obligations under the bill, and authorizes controllers to report compliance metrics on their public websites.

(24) Provides that a controller may only engage in processing with the consent of the consumer if a risk assessment determines that potential risks of privacy harm outweigh the interests of the controller, consumer, other stakeholders, and the public.

(25) Sets forth additional circumstances when processing data for business purposes, as described in a risk assessment, is not presumed permissible.

(26) Requires controllers or processors that use, sell, or share deidentified data to make a public commitment not to reidentify

deidentified data, to take certain steps to prevent reidentification of that data by third parties and to address any breaches of contractual commitments to which deidentified data is subject.

(27) Eliminates certain exemptions and sets forth additional circumstances that may exempt a controller or processor from the obligations set forth in the bill.

(28) Authorizes the Office of Privacy and Data Protection to grant one-year waivers to permit processing for certain purposes.

(29) Prohibits controllers from selling any personal data processed pursuant to an exemption or a waiver.

(30) Removes provisions related to limiting a controller's or processor's liability when disclosing personal data to third-party controllers or processors in specified circumstances.

(31) Sets forth additional requirements for controllers and processors that use or provide facial recognition services.

(32) Provides that the obligations related to facial recognition technology do not restrict a controller's or processor's ability to prevent, detect, or respond to security incidents, or to protect against theft, fraud, or other malicious or deceptive activities.

(33) Modifies the requirements related to state and local government agencies' use of facial recognition.

(34) Modifies the enforcement provisions by providing that a violation of the bill is an unfair or deceptive act for the purpose of applying the Consumer Protection Act.

(35) Modifies the rule-making authorization for the Office of Privacy and Data Protection, including changing the date of a report on the public and private sector use of facial recognition.

(36) Directs the Office of Privacy and Data Protection to conduct a study and to report to the Legislature on whether certain federal health information laws adequately protect personal health information and prevent it from being bought, sold, or traded on a commercial basis.

(37) Directs the Office of Privacy and Data Protection to convene a work group and to report to the Legislature regarding the best practices for ensuring consumers understand their privacy rights prior to agreeing to Terms of Service, Terms of Agreement, and other similar documents.

(38) Modifies the effective date of the bill from July 31, 2021, to July 30, 2020, except for the section related to the Office of Privacy and Data Protection, which takes effect 90 days after final adjournment of the legislative session in which this act is enacted.

--- END ---