2SSB 5062 - H AMD **539**
By Representative Kloba

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.

NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS AND INTENT. (1) The legislature finds that the people of Washington regard their privacy as a fundamental right and an essential element of their individual freedom. Washington's Constitution explicitly provides the right to privacy, and fundamental privacy rights have long been and continue to be integral to protecting Washingtonians and to safeguarding our democratic republic.

(2) Ongoing advances in technology have produced an exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed, which presents both promise and potential peril. The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society. However, it has also created risks to privacy and freedom. The unregulated and unauthorized use and disclosure of personal information and loss of privacy can have devastating impacts, ranging from financial fraud, identity theft, and unnecessary costs, to personal time and finances, to destruction of property, harassment, reputational damage, emotional distress, and physical harm.

(3) Given that technological innovation and new uses of data can help solve societal problems, protect public health associated with global pandemics, and improve quality of life, the legislature seeks to shape responsible public policies where innovation and protection of individual privacy coexist. The legislature notes that our federal authorities have not developed or adopted into law regulatory or legislative solutions that give consumers control over their privacy. In contrast, the European Union's general data protection regulation has continued to influence data privacy policies and practices of

those businesses competing in global markets. In the absence of federal standards, Washington and other states across the United States are analyzing elements of the European Union's general data protection regulation to enact state-based data privacy regulatory protections.

(4) With this act, the legislature intends to: Provide a modern privacy regulatory framework with data privacy guardrails to protect individual privacy; establish mechanisms for consumers to exercise control over their data; and require companies to be responsible custodians of data as technological innovations emerge.

(5) This act gives consumers the ability to protect their own rights to privacy by explicitly providing consumers the right to access, correct, and delete personal data, as well as the rights to obtain data in a portable format. These rights will add to, and not subtract from, the consumer protection rights that consumers already have under Washington state law.

(6) This act also imposes affirmative obligations upon companies to safeguard personal data, and provide clear, understandable, and transparent information to consumers about how their personal data is used. It strengthens compliance and accountability by requiring data protection assessments in the collection and use of personal data. Finally, it empowers the state attorney general to obtain and evaluate a company's data protection assessments, to conduct investigations, while preserving consumers' rights under the consumer protection act to impose penalties where violations occur, and to prevent against future violations.

NEW SECTION. **Sec. 101.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, that other legal entity. For these purposes, "control" or "controlled" means: Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(2) "Air carriers" has the same meaning as defined in the federal aviation act (49 U.S.C. Sec. 40101, et seq.), including the airline deregulation act (49 U.S.C. 41713).

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 104 (1) through (4) of this act is being made by the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(4) "Biometric information" means a record of one or more measurable biological or behavioral characteristics that can be used alone or in combination with each other or with other information for automated recognition of a known or unknown individual. Examples include but are not limited to: Fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, gait, handwriting, key stroke dynamics, and mouse movements. Biometric information does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric information does not include donated organs, tissues, or parts, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric information does not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996. Biometric information does not include an X-ray, roentgen process, computed tomography, magnetic resonance imaging, positron emission tomography scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

(5) "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.

(6) "Child" has the same meaning as defined in the children's online privacy protection act, Title 15 U.S.C. Sec. 6501 through 6506.

(7) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer

signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through dark patterns does not constitute consent.

(8) "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.

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

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

(11) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(12) "Decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

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

(14) "Device" means a tool that is capable of sending, routing, or receiving communications to or from another device and intended

for use by a single consumer or single household or, if used outside of a home, for use by the general public.

(15) "Harm" means any potential or realized adverse consequences to a consumer or to society, including but not limited to:

(a) Direct or indirect financial harm;

(b) Physical harm or threats to consumers or property, including but not limited to bias-related crimes and threats, harassment, and sexual harassment;

(c) Discrimination in products, services, or economic opportunity, such as housing, employment, credit, insurance, education, or health care, on the basis of a consumer's or class of consumers' actual or perceived age, race, national origin, sex, sexual orientation, gender identity, disability, and/or membership in another protected class, except as specifically authorized by law;

(d) Interference with or surveillance of First Amendment protected activities by state actors, except as specifically authorized by law;

(e) Interference with the right to vote or with free and fair elections;

(f) Violation of consumers' rights to due process or equal protection under the law;

(g) Loss of individual control over personal data via nonconsensual sharing of private information, data breach, or other actions that violate the rights listed in section 104 of this act;

(h) The nonconsensual capture of information or communications within a consumer's home or where the consumer is entitled to have a reasonable expectation of privacy or access control; and

(i) Other effects on a consumer that may not be reasonably foreseeable to, contemplated by, or expected by the consumer to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller, and that alter or limit that consumer's choices or predetermines results.

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

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

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

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

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

(21) "Judicial branch" means any court, agency, commission, or department provided in Title 2 RCW.

(22) "Known child" means a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's age.

(23) "Legislative agencies" has the same meaning as defined in RCW 44.80.020.

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

(25) "Minor" means an individual who is at least 13 and under 16 years of age under circumstances where a controller has actual knowledge of, or willfully disregards, the minor's age.

(26) "Monetize" means to sell, rent, release, disclose, disseminate, trade, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a consumer's personal data by a controller, processor, or a third party in exchange for monetary or other consideration, as well as to leverage or use a consumer's personal data to place a targeted advertisement or to otherwise profit, regardless of whether the consumer's personal data changes hands.

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

(28) "Personal data" means any information, including pseudonymous data, that is linked or reasonably linkable to an identified or identifiable natural person who is a Washington resident and that is captured in an interaction in which a controller directly or indirectly makes available information, products, or services to a consumer or household. Covered interactions include but are not limited to posting of information, offering of a product or service, the placement of targeted advertisements, or offering a membership or other ongoing relationship with an entity. For the purposes of this chapter, "personal data" includes biometric information, regardless of how captured.

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

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

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

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

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

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

(35)(a) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party or to otherwise profit, regardless of whether the consumer's personal data changes hands.

(b) "Sale" does not include the following: (i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of information that the consumer (A) intentionally made available to the general public via a channel of mass media, and (B) did not restrict to a specific audience; or (v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(36) "Sensitive data" means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the

purpose of uniquely identifying a natural person; (c) the personal data from a known child; or (d) specific geolocation data. "Sensitive data" is a form of personal data.

(37) "Specific geolocation data" means information derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms that directly identifies the specific location of a natural person within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet. Specific geolocation data excludes the content of communications.

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

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

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

(41) "Washington governmental entity" means a department or agency of Washington state or a political subdivision thereof, including but not limited to public authorities and special use districts, or an individual acting for or on behalf of the state or a political subdivision thereof.

NEW SECTION. **Sec. 102.** JURISDICTIONAL SCOPE. (1) This chapter applies to legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) During a calendar year, processes the personal data of 1,000 or more unique consumers; or

(b) Processes personal data and earns or receives $10,000,000 or more of annual revenue through 300 or more transactions.

(2) This chapter does not apply to:

(a) State agencies, legislative agencies, the judicial branch, local governments, or tribes, except as provided in sections 108 and 113 of this act;

(b) Municipal corporations, except as provided in sections 108 and 113 of this act;

(c) Air carriers;

(d) Nonprofit organizations that:

(i) Are registered with the secretary of state under the charities program pursuant to chapter 19.09 RCW;

(ii) Collect personal data during legitimate activities related to the organization's tax-exempt purpose; and

(iii) Do not sell personal data collected by the organization;

(e) Information that meets the definition of:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(j) 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;

(k) 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;

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

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

(n) Personal data collected, maintained, disclosed, or otherwise used in connection with the gathering, dissemination, or reporting of news or information to the public by news media as defined in RCW 5.68.010(5);

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

(p) Data collected or maintained: (i) In the course of an individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that it is collected and used solely within the context of that role; (ii) as the emergency contact information of an individual under (p)(i) of this subsection used solely for emergency contact purposes; or (iii) that is necessary for the business to retain to administer benefits for another individual relating to the individual under (p)(i) of this subsection is used solely for the purposes of administering those benefits.

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

(4) Payment-only credit, check, or cash transactions where no data about consumers are retained do not count as "consumers" for purposes of subsection (1) of this section.

NEW SECTION. **Sec. 103.** OPT-IN CONSENT. (1) A controller may not, without freely given, specific, informed, and unambiguous opt-in consent from a consumer:

(a) Process the consumers personal data; or

(b) Make any changes in the processing of the consumer's personal data that would necessitate a change to the privacy notice required to be provided under section 110 of this act.

(2) For continuing interactions, whether by automatic renewal or nontime-limited interactions, the opt-in consent required by this section must be renewed not less than annually, and if not so renewed shall be deemed to have been withdrawn.

(3) A controller requesting consent shall ensure that the option to withhold consent is presented as clearly and prominently as the option to provide consent.

(4) A controller shall provide a mechanism for a consumer to withdraw previously given consent at any time. The consumer must be notified when the withdrawal of consent is complete. It must be as easy for a consumer to withdraw consent as it is to provide consent.

(5) Under no circumstances shall a consumer's interaction with a controller's product or service when the controller has a terms of service or a privacy policy in and of itself constitute freely given, specific, informed, and unambiguous consent.

(6) To the extent that a controller must process internet protocol addresses, system configuration information, uniform resource locators of referring pages, locale and language preferences, keystrokes, and other personal data in order to obtain a consumer's freely given, specific, informed, and unambiguous opt-in consent, the controller shall:

(a) Process only the personal data necessary to request freely given, specific, informed, and unambiguous opt-in consent;

(b) Process the personal data solely to request freely given, specific, informed, and unambiguous opt-in consent; and

(c) Immediately delete the personal data if consent is not given.

(7) A controller shall not refuse to serve a consumer who does not approve the processing of the consumer's personal data under this section unless the processing is necessary for the primary purpose of the transaction that the consumer has requested.

(8) A controller shall not discriminate against consumers by reason of their not granting opt-in consent to the processing of their personal data under this chapter or otherwise exercising their

rights under this chapter, including but not limited to, by: Denying goods or services to the consumer; charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; providing a different level or quality of goods or services to the consumer; and suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. Notwithstanding this subsection, a controller may, with the consumer's opt-in consent given in compliance with this section, operate a program in which information, products, or services sold to the consumer are discounted based on that consumer's prior purchases from the controller, provided that the personal data shall be processed solely for the purpose of operating such program.

(9) A controller shall not state or imply that the quality of a product or service will be diminished and shall not actually diminish the quality of a product or service if the consumer declines to give opt-in consent to personal data processing.

(10) The Washington state department of commerce is hereby authorized and directed to conduct a study to determine the most effective way for controllers to obtain the consumers' freely given, specific, informed, and unambiguous opt-in consent for each type of personal data processing. The Washington state department of commerce may request data and information from controllers conducting business in Washington state, other Washington state government entities administering notice and consent regimes, consumer protection experts, privacy advocates, researchers, internet standards setting bodies such as the internet engineering task force and institute of electrical and electronics engineers, and other relevant sources to meet the purpose of the study.

(11) Within six months of enactment of this act, the Washington state department of commerce shall adopt regulations specifying how:

(a) Controllers must notify consumers of their rights under this chapter and obtain the consumers' freely given, specific, informed, and unambiguous opt-in consent for each use model of personal data processing; and

(b) Controllers must notify consumers of their right to withdraw their consent at any time and how the right may be exercised.

(12) Within six months of enactment of this act, the Washington state department of commerce shall adopt regulations grouping different types of processing of personal data by use model and

permitting a controller to simultaneously obtain freely given, specific, informed, and unambiguous opt-in consent from a consumer for multiple transactions of the same use model.

NEW SECTION. **Sec. 104.** CONSUMER RIGHTS. (1) A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access the personal data the controller is processing.

(2) A consumer has the right to correct inaccurate personal data concerning the consumer.

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

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

(5) A consumer has the right to refuse consent for any processing of the consumer's personal data that is not essential to the primary transaction.

NEW SECTION. **Sec. 105.** EXERCISING CONSUMER RIGHTS. (1) A consumer may exercise the rights set forth in section 104 of this act by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise.

(2) In the case of processing personal data of a known child, the parent or legal guardian of the known child may exercise the rights of this chapter on the child's behalf.

(3) In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under chapter 11.88, 11.92, or 11.130 RCW, the guardian or the conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

NEW SECTION. **Sec. 106.** RESPONDING TO REQUESTS. (1) Except as provided in this chapter, the controller must comply with a request to exercise the rights pursuant to section 104 of this act.

(2)(a) Controllers must provide one or more secure and reliable means for consumers to submit a request to exercise their rights

under this chapter. These means must take into account the ways in which consumers interact with the controller and the need for secure and reliable communication of the requests.

(b) Controllers may not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this chapter.

(3)(a) A controller must inform a consumer of any action taken on a request to exercise any of the rights in section 104 (1) through (4) of this act without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 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 45 days of receipt of the request, together with the reasons for the delay.

(b) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subsection (4) of this section.

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

(d) A controller is not required to comply with a request to exercise any of the rights under section 104 (1) through (4) of this act if the controller is unable to authenticate the request using commercially reasonable efforts. In such a case, the controller may request the provision of additional information reasonably necessary to authenticate the request.

(4)(a) A controller must establish an internal process whereby a consumer may appeal a refusal to take action on a request to exercise any of the rights under section 104 of this act within a reasonable period of time after the controller refuses to take action on such request.

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

(c) Within 30 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of such an extension within 30 days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to (c) of this subsection, the controller must clearly and prominently provide the consumer with information about how to file a complaint with the consumer protection division of the attorney general's office. The controller must maintain records of all such appeals and how it responded to them for at least 24 months and shall, upon request, compile and provide a copy of such records to the attorney general.

NEW SECTION. **Sec. 107.** SURREPTITIOUS SURVEILLANCE. (1) A consumer has the right to not be subject to surreptitious surveillance.

(2) A controller may not activate the microphone, camera, or any other sensor on a device in the lawful possession of a consumer that is capable of collecting or transmitting personal data, without providing the privacy notice required in section 110 of this act and obtaining the consumer's freely given, specific, informed, and unambiguous opt-in consent pursuant to section 103 of this act for the specific type of measurement to be activated; provided that such opt-in consent shall be effective for no more than 90 days after which it shall expire unless renewed by the consumer's freely given, specific, informed, and unambiguous opt-in consent pursuant to section 103 of this act.

NEW SECTION. **Sec. 108.** BIOMETRIC INFORMATION. In addition to all provisions of this chapter applicable to personal data, the following provisions are applicable to all biometric information, regardless of how such biometric information is processed.

(1) Retention; disclosure; destruction. A controller or Washington governmental entity that processes biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for processing such information has been satisfied or within one year of the consumer's last interaction with the controller or Washington governmental entity, whichever occurs first. Consent under subsection (2) of this section shall be for a period specified in the written consent of not more than one year, and shall automatically expire at the end of such period unless renewed pursuant to subsection (2) of this section. Upon expiration of consent, any biometric information possessed by a controller or Washington governmental entity must be destroyed. Absent a valid warrant issued by a court of competent jurisdiction, a controller or Washington governmental entity in possession of biometric information must comply with its established retention schedule and destruction guidelines.

(2) Processing. A controller or Washington governmental entity may not process a consumer's biometric information, unless it first:

(a) Informs the consumer in writing that biometric information is being processed;

(b) Informs the consumer in writing the details of the specific purpose or purposes and length of term for which biometric information is processed; and

(c) Receives a freely given, specific, informed, and unambiguous written opt-in consent executed by the consumer specifically authorizing such processing.

(3) Disclosure. No controller or Washington governmental entity in possession of biometric information may disclose or otherwise disseminate a consumer's biometric information unless:

(a) The consumer gives freely given, specific, informed, and unambiguous opt-in consent in writing to the disclosure or redisclosure;

(b) The disclosure or redisclosure is used solely to complete a financial transaction requested or authorized by the subject of the biometric information;

(c) The disclosure or redisclosure is required by state or federal law; or

(d) The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction or a subpoena issued by a governmental entity or in a pending judicial case, provided that in the case of a subpoena the entity subject to the subpoena shall postpone compliance therewith until it has given the subject of the subpoena notice of the facts set forth in section 113(2)(b)(i) of this act and has allowed at least 10 business days for the subject to seek review of or otherwise challenge the subpoena.

(4) Monetizing. A controller or Washington governmental entity in possession of biometric information may not monetize, or otherwise profit from a consumer's biometric information; provided only that a controller may process a consumer's biometric information, with full disclosure and opt-in consent consistent with section 103 of this act, in a service in which the controller reports to the consumer the biometric information processed or utilizes the biometric information to design or recommend actions or products that have been specifically requested by the consumer with full disclosure that such recommendation is based on the biometric information processed, provided that the biometric information shall not be used for any other purpose.

(5) Identification. Notwithstanding any other provision of this chapter, a controller or Washington governmental entity may list personal data such as name or birthdate and biometric information such as height, weight, or photograph on an issued license or membership or identification card for the sole purpose of allowing an employee or other representative of the controller or Washington governmental entity to determine based solely on personal observation, and without the assistance of technologies such as facial recognition, whether the person physically holding such license or card is the person entitled to hold it, provided further that such intended use is disclosed to the consumer prior to capturing the biometric information. Any other processing of such biometric information shall be subject to all the terms and conditions of this chapter. Any controller or governmental entity using personal information or biometric information under this subsection must ensure that it is not stored or processed in any

manner that would allow a third party to process such information for any purpose.

(6) Consent to processing information pursuant to the protocols for human experimentation constitutes freely given, specific, informed, and unambiguous opt-in consent under this section.

NEW SECTION. **Sec. 109.** RESPONSIBILITY ACCORDING TO ROLE. (1) Controllers and processors are responsible for meeting their respective obligations established under this chapter.

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

(a) Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 104 of this act; and

(b) Taking into account the nature of processing and the information available to the processor, the processor shall: Assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to RCW 19.255.010; and provide information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 112 of this act. The controller and processor are each responsible for only the measures allocated to them.

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

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

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

(4) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and

organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement such measures.

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

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

(b)(i) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and

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

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

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

with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to the processing.

NEW SECTION. **Sec. 110.** RESPONSIBILITIES OF CONTROLLERS. (1)(a) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

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

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

(iii) How and where consumers may exercise the rights contained in section 104 of this act, including how a consumer may appeal a controller's action with regard to the consumer's request;

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

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

(b) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing.

(c) The privacy notice required under this subsection must:

(i) Use clear and plain language;

(ii) Be in English and any other language in which a controller communicates with the consumer to whom the information pertains; and

(iii) Be understandable to the least sophisticated consumer.

(2) A controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which the data is processed.

(3) A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which the data is processed.

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

(5) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and

accessibility of personal data. The data security practices must be appropriate to the volume and nature of the personal data at issue.

(6) A controller shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability, in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: (a) Housing; (b) employment; (c) credit; (d) education; or (e) the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.

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

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

NEW SECTION. **Sec. 111.** PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA. (1) This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:

(a) Reidentify deidentified data;

(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data pursuant to section 104 (1) through (4) of this act, if all of the following are true:

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

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

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

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

(2) The rights contained in section 104 of this act do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

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

NEW SECTION. **Sec. 112.** DATA PROTECTION ASSESSMENTS. (1) Controllers must conduct and document a data protection assessment of each of the following processing activities involving personal data:

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

(b) The processing of personal data for the purposes of the sale of personal data;

(c) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or disparate impact on, consumers;

(ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

(d) The processing of sensitive data; and

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

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

(2) Data protection assessments conducted under subsection (1) of this section must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, must be factored into this assessment by the controller.

(3) The attorney general may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data protection assessments for compliance with the responsibilities contained in section 110 of this act and, if it serves a civil investigative demand, with RCW 19.86.110. Data protection assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment unless otherwise subject to case law regarding the applicability of attorney-client privilege or work product protections.

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

NEW SECTION. **Sec. 113.** EXCEPTIONS TO THE CONSENT REQUIREMENT. (1) With respect to personal data that is not biometric information, a controller is not required to obtain freely given, specific, informed, and unambiguous opt-in consent from a consumer under section 103 of this act if the processing is necessary to execute the specific transaction for which the consumer is providing personal data, such as the provision of financial information to complete a purchase or the provision of a mailing address to deliver a package. However, personal data shall not be processed for any other purpose beyond that clear primary purpose without the freely given, specific, informed, and unambiguous opt-in consent from the consumer to whom the personal data pertains, except as required by law.

(2) With respect to personal data generally, a controller or Washington governmental entity is not required to obtain freely given, specific, informed, and unambiguous opt-in consent from a consumer under section 103 or 108(1) of this act if:

(a) It believes that an emergency involving immediate danger of death or serious physical injury to any consumer requires obtaining without delay personal data related to the emergency and the request is narrowly tailored to address the emergency, subject to the following limitations:

(i) The request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to a consumer requires obtaining without delay personal data relating to the emergency; and

(ii) Simultaneous with the controller or Washington governmental entity obtaining personal data under this subsection (2)(a), the controller or Washington governmental entity shall use reasonable efforts to inform the consumer of the personal data obtained; the details of the emergency; and the reasons why the controller or Washington governmental entity needed to use, access, or disclose the biometric information and shall continue such efforts to inform until receipt of information is confirmed; and

(b) Disclosure is required to respond to a warrant or subpoena issued by a court of competent jurisdiction or a subpoena issued by a governmental entity or pursuant to a pending judicial proceeding:

(i) Unless a delayed notice is ordered, both the entity requesting the warrant or subpoena and any entity receiving such warrant or subpoena shall, simultaneous with requesting or receiving a warrant compelling disclosure of or serving or receiving a subpoena for personal data, serve or deliver the following information to the subject of the warrant or subpoena by registered or first-class mail, email, or other means reasonably calculated to be effective:

(A) A copy of the warrant or subpoena and notice that informs the consumer of the nature of the inquiry with reasonable specificity;

(B) That personal data maintained for the consumer was supplied to or requested by the requesting entity and the date on which the supplying or request took place;

(C) An inventory of the personal data requested or supplied; and

(D) The identity of the entity or individual from which the information is requested.

(ii) A controller or Washington governmental entity acting under (d) of this subsection may apply to the court for an order delaying notification, and the court may issue the order if the court determines that there is reason to believe that notification of the existence of the warrant will result in endangering the life or physical safety of a consumer, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(iii) In the case of a subpoena, a controller subject to a subpoena shall postpone compliance therewith until it has given the subject of the subpoena notice of the information required under (b)(i) of this subsection and has allowed at least 10 business days for the subject to seek review of or otherwise challenge the subpoena;

(c) The disclosure is required by state or federal law; or

(d) Processing involves only deidentified information.

(3) This chapter shall not apply to personal data captured from a patient by a health care provider or health care facility as defined in RCW 48.41.030 or biometric information collected, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, insurance, payment, or operations under the federal health insurance portability and accountability act of 1996, or to X-ray, roentgen process, computed tomography, magnetic resonance imaging, positron emission tomography

scan, mammography, or other image or film of the human anatomy used exclusively to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

(4) To the extent the transaction requested by a consumer is a controller's placement of that consumer's personal data in the public domain, such as recording of a real estate deed showing name and address, the controller has the same rights as any other person or entity with regard to such information.

(5) This chapter does not apply to consumers sharing their personal contact information such as email addresses with other consumers in workplace, social, political or similar settings where the purpose of the information is to facilitate communication among such consumers, provided that any processing of such contact information beyond interpersonal communication is covered by this chapter. This chapter shall not apply to controllers' publication of controller-based member or employee contact information where such publication is intended to allow members of the public to contact such member or employee in the ordinary course of the controller's operations.

(6) Nothing in this chapter diminishes any consumer's or controller's rights or obligations under chapter 70.02 RCW.

NEW SECTION. **Sec. 114.** LIMITATIONS AND APPLICABILITY. (1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

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

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

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

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

(e) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or

take steps at the request of the consumer prior to entering into a contract;

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

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

(h) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines: (i) If the research is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

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

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

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

(b) Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party when those internal operations are performed during, and not following, the consumer's relationship with the controller.

(3) The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under Washington law and do not prevent a controller or processor

from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Washington law as part of a privileged communication.

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

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

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

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

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

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (8) of this section.

(8)(a) Personal data that is processed by a controller pursuant to this section must not be processed for any purpose other than those expressly listed in this section.

(b) Personal data that is processed by a controller pursuant to this section may be processed solely to the extent that such processing is: (i) Necessary, reasonable, and proportionate to the purposes listed in this section; (ii) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section; and (iii) insofar as possible, taking into account the nature and purpose of processing the personal data, subjected to reasonable administrative, technical, and physical

measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers.

NEW SECTION. **Sec. 115.** PRIVATE RIGHT OF ACTION. (1) Any consumer alleging a violation of this chapter or a regulation adopted under this chapter may bring a civil action in any court of competent jurisdiction. A consumer protected by this chapter may not be required, as a condition of service or otherwise, to accept mandatory arbitration of a claim under this chapter.

(2) A violation of this chapter or a regulation adopted under this chapter with respect to the personal data of a consumer constitutes a rebuttable presumption of harm to that consumer.

(3) In a civil action in which the plaintiff prevails, the court may award:

(a) Liquidated damages of $10,000 per violation or actual damages, whichever is greater;

(b) Punitive damages; and

(c) Any other relief, including but not limited to an injunction, that the court determines appropriate.

(4) In addition to any relief awarded pursuant to subsection (3) of this section, the court shall award reasonable attorneys' fees and costs to any prevailing plaintiff.

NEW SECTION. **Sec. 116.** ENFORCEMENT. (1) 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. In actions brought by the attorney general, the legislature finds: (a) 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, and (b) a violation of this chapter is not reasonable in relation to the development and preservation of business, 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) Until July 31, 2023, in the event of a controller's or processor's violation under this chapter, prior to filing a complaint, the attorney general must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the attorney general alleges have been or are being

violated. If, after 30 days of issuance of the warning letter, the attorney general believes the controller or processor has failed to cure any alleged violation, the attorney general may bring an action against the controller or processor as provided under this chapter.

(3) Beginning July 31, 2023, in determining a civil penalty under this chapter, the court must consider, as mitigating factors, a controller's or processor's good faith efforts to comply with the requirements of this chapter and any actions to cure or remedy the violations before an action is filed.

(4) All receipts from the imposition of civil penalties under this chapter must be deposited into the consumer privacy account created in section 117 of this act.

NEW SECTION. **Sec. 117.** CONSUMER PRIVACY ACCOUNT. The consumer privacy account is created in the state treasury. All receipts from the imposition of civil penalties under this chapter must be deposited into the account. Moneys in the account may be spent only after appropriation. Moneys in the account may only be used for the purposes of recovery of costs and attorneys' fees accrued by the attorney general in enforcing this chapter and for the office of privacy and data protection as created in RCW 43.105.369. Moneys may not be used to supplant general fund appropriations to either agency.

NEW SECTION. **Sec. 118.** 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. 119.** A new section is added to chapter 42.56 RCW to read as follows:

Data protection assessments submitted by a controller to the attorney general in accordance with requirements under section 112 of this act are exempt from disclosure under this chapter.

NEW SECTION. **Sec. 120.** A new section is added to chapter 44.28 RCW to read as follows:

(1) By December 1, 2023, the joint committee must review the efficacy of the attorney general providing controllers and processors with warning letters and 30 days to cure alleged violations in the warning letters pursuant to section 116 of this act and report its

findings to the governor and the appropriate committees of the legislature.

(2) The report must include, but not be limited to:

(a) The number of warning letters the attorney general sent to controllers and processors;

(b) A list of the controller and processor names that received the warning letters;

(c) The categories of violations and the number of violations per category;

(d) The number of actions brought by the attorney general as authorized in this act due to a controller or processor not curing the alleged violations within 30 days;

(e) The types of resources, including associated costs, expended when providing warning letters and tracking compliance; and

(f) A recommendation on whether the warning letters provided by the attorney general should be continued.

(3) The office of the attorney general shall provide the joint committee any data within their purview that the joint committee considers necessary to conduct the review.

(4) This section expires June 30, 2024.

NEW SECTION. **Sec. 121.** Sections 101 through 117 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 122.** Sections 1, 2, and 101 through 120 of this act take effect July 31, 2022.

NEW SECTION. **Sec. 123.** Sections 101 through 117 of this act do not apply to institutions of higher education or nonprofit corporations until July 31, 2026."

Correct the title.

EFFECT: Strikes Part 2 and Part 3 of the bill relating to the processing of data collected by private and public entities for certain public health emergency and contact tracing purposes. Removes provisions related to the stricken parts of the bill from the legislative intent section.

Makes the following changes in Part 1 of the bill relating to consumer personal data privacy:

Key Definitions and Jurisdictional Scope:

(1) Adds the definitions of "biometric information," "device," "harm," "monetize," and "Washington governmental entity."

(2) Modifies the definition of "deidentified data" to require that controllers take reasonable measures to ensure that the data cannot be associated not only with a natural person, but also with a household or device.

(3) Specifies that exchanging personal data for monetary or other valuable consideration or otherwise profiting constitutes "sale" regardless of whether the consumer's personal data changes hands.

(4) Modifies the definition of "targeted advertising" to mean displaying advertisements selected on the basis of a consumer's activities across one or more distinctly branded websites, rather than across nonaffiliated websites. Specifies that targeted advertising does not include advertising based on activities within a controller's own commonly branded websites, rather than a controller's own websites.

(5) Applies the requirements of the bill to legal entities that, during a calendar year, process the personal data of at least 1,000 consumers, rather than 100,000 consumers, or that earn $10,000,000 in annual revenue through at least 300 transactions, rather than derive 25 percent of gross revenue from the sale of data.

(6) Provides that state agencies, legislative agencies, judicial branch, local governments, tribes, and municipal corporations are not exempt from the provisions related to biometric information.

(7) Exempts from the bill nonprofit organizations that are registered with the Secretary of State under the Charities Program, collect personal data during legitimate activities related to the organization's tax-exempt purpose, and do not sell personal data collected by the organization.

Opt-in Consent:

(8) Requires controllers to obtain a consumer's opt-in consent before processing the consumer's personal data or making any changes in the processing that would necessitate a change to the required privacy notice.

(9) Requires the opt-in consent to be renewed not less than annually and the option to withhold consent to be presented as clearly and prominently as the option to provide consent.

(10) Requires controllers to provide a mechanism to withdraw consent at any time.

Privacy Notice:

(11) Requires the privacy notice to use clear and plain language and to be understandable to the least sophisticated consumer, as well as be in English and any other language in which a controller communicates with the consumer to whom the information pertains.

Consumer Rights:

(12) Provides that a consumer has the right to access the personal data a controller is processing, rather than the right to access the categories of personal data a controller is processing.

(13) Strikes from the right to correct inaccurate personal data the requirement to take into consideration the nature of the personal data and the purposes of processing.

(14) Removes the right to opt out of the processing for certain purposes and instead provides that a consumer has the right to refuse consent for any processing of the consumer's personal data.

(15) Strikes provisions related to opting out of processing via global privacy controls or by designating an authorized agent.

(16) Provides that a controller must respond to a request to exercise the right to access personal data within 45 days of receiving the request.

(17) Provides that a consumer has the right to not be subject to surreptitious surveillance and prohibits controllers from activating a microphone, camera, or any other sensor capable of collecting or

transmitting personal data without first providing the required privacy notice and obtaining opt-in consent, which is to expire after 90 days unless renewed by the consumer.

Biometric Information:

(18) Defines the obligations of controllers and Washington governmental entities relating to biometric information, including: Informing consumers that biometric information is being processed; obtaining opt-in consent; establishing retention schedules and guidelines for permanently destroying biometric information; disclosing biometric information only if specified circumstances exist; and prohibiting monetization of biometric information unless limited exceptions apply.

Exceptions to the Consent Requirement:

(19) Specifies the circumstances when controllers and Washington governmental entities are not required to obtain opt-in consent for processing of personal data or biometric information, including: Processing is necessary to execute the specific transaction requested by a consumer; in cases of emergency, if specified requirement are met; disclosure is required by state or federal law or to respond to a warrant or subpoena, if specified requirements are met; or processing involves only deidentified information.

(20) Exempts certain health-related personal data and biometric information, as well as the sharing of personal contact information by consumers for purposes of interpersonal communication.

Private Right of Action:

(21) Strikes the provisions that bar a private right of action in the underlying bill and instead provides that a consumer alleging a violation may bring a civil action and recover liquidated damages of $10,000 per violation or actual damages, whichever is greater, punitive damages, and any other relief that the court determines appropriate.

(22) Requires the court to award reasonable attorneys' fees and costs to any prevailing plaintiff.

Enforcement by the Attorney General:

(23) Expires the right to cure violations one year after the effective date of the bill.

(24) Removes the statutory penalties from the provisions related to enforcement by the Attorney General and instead provides that after the expiration of the right to cure, when determining a civil penalty, the court must consider a controller's or processor's good faith efforts to cure as mitigating factors.

Preemption:

(25) Removes the provisions that preempt local laws and regulations regarding the processing personal data.

Studies and Reports:

(26) Directs the Department of Commerce to conduct a study to determine the most effective way for controllers to obtain consumers' consent and adopt regulation related to opt-in consent.

(27) Requires the Joint Legislative Audit and Review Committee study on the efficacy of the Attorney General providing warning letters to controllers and processors to be completed by December 1, 2023, rather than December 1, 2025.

(28) Strikes the provisions requiring the Office of Privacy and Data Protection to complete a study and submit a report on the

development of technology related to opting out of the processing of personal data.

--- END ---