S-1018.1

SENATE BILL 5643

State of Washington 68th Legislature 2023 Regular Session

By Senator Hasegawa

AN ACT Relating to creating a charter of people's personal data rights; adding a new section to chapter 42.56 RCW; adding a new chapter to Title 19 RCW; creating a new section; prescribing penalties; and providing an effective date.

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

NEW SECTION. **Sec. 1.** This act may be known and cited as the people's privacy act.

NEW SECTION. **Sec. 2.** The legislature finds that:

(1) Washingtonians have an explicit right to privacy under Article I, section 7 of the Washington state Constitution and this act furthers protection of that fundamental constitutional right.

(2) Advances in technology and the rapid growth in the volume and variety of personal information being generated, collected, stored, and analyzed have increased harms to individual and collective privacy, making the protection of this vital right a matter of urgency.

(3) Privacy violations and misuse of personal information in the digital age can lead to a range of harms, including discrimination in employment, health care, housing, access to credit, and other areas; unfair price discrimination; domestic violence; abuse; stalking;

harassment; entrapment; and financial, emotional, and reputational harms.

(4) Privacy harms disproportionately affect low-income people and people of color.

(5) Privacy violations not only threaten the fundamental rights and privileges of Washingtonians, but they also menace the foundation and supporting institutions of a free democratic state.

(6) Washingtonians are increasingly required to share personal information and are subjected to automated forms of surveillance and classification as a consequence of simply participating in public life and accessing basic social goods, services, and opportunities.

(7) Entities that collect, use, retain, share, and monetize personal information have specialized knowledge about the algorithms and data security measures they use, as well as information about how they collect, use, retain, share, and monetize personal information that the average individual is unlikely to understand. Just as banks, lawyers, and medical providers, given their specialized knowledge, have special obligations to individuals, entities collecting intimate personal information in the digital age and benefiting from similarly specialized knowledge should have similar obligations.

(8) Privacy is the foundation of consumer trust, particularly in electronic commerce, and people will use advanced data-driven technology only if their privacy rights are respected, their personal information is safeguarded, and their freedom to choose how much personal information to share is unobstructed.

(9) The state of Washington is more protective of personal privacy than many other states and has an obligation to ensure that its residents can control their personal information and are able to understand and regulate how that personal information may be used by others.

(10) Requiring entities to obtain opt-in consent prior to the use or disclosure of personal information is essential to protecting personal privacy. Without opt-in consent, individuals who wish to control their personal information face an insurmountable challenge of identifying and engaging with each and every entity they encounter, while businesses lack the incentive to present individuals with meaningful opportunities to choose. An opt-in approach gives people meaningful control over their personal information while allowing businesses to choose how and whether they request consent to process that information.

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

(1) "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.

(2) "Captured personal information" means personal information about a Washington resident that is captured in an interaction in which a covered entity directly or indirectly makes available information, products, or services to an individual 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, "captured personal information" includes biometric information, regardless of how captured.

(3) "Collect" means to buy, rent, gather, obtain, receive, trade for, or access any personal information pertaining to an individual

by any means, online or offline, including but not limited to receiving information from the individual or from a third party, actively or passively, or obtaining information by observing the individual's behavior.

(4) "Conduct business in Washington" or "conducting business in Washington" means to produce, solicit, or offer for use or sale any information, product, or service in a manner that intentionally targets, or may reasonably be expected to contact natural persons located in Washington state, whether or not for profit.

(5) "Covered entity" means a person or legal entity that is not a governmental entity and that conducts business in Washington state, processes captured personal information, and (a) has earned or received $10,000,000 or more of annual revenue through 300 or more transactions or (b) processes and/or maintains the captured personal information of 1,000 or more unique individuals during the course of a calendar year.

(6) "Data processer" means a person or legal entity that processes captured personal information on behalf of a covered entity.

(7) "Deidentified" means captured personal information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household, provided that a covered entity that uses deidentified captured personal information must:

(a) Implement technical safeguards that prohibit reidentification of the information;

(b) Implement business processes that specifically prohibit reidentification of the information;

(c) Implement business processes that prevent inadvertent release of deidentified information;

(d) Not attempt to reidentify the information; and

(e) Contractually obligate any recipients of the information to comply with all the provisions of this subsection.

If a covered entity intentionally shares any deidentified captured personal information, it shall condition such sharing on the agreement by any recipients to abide by the same restrictions and to submit to jurisdiction under this chapter in any action based on violation of such restrictions.

(8) "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 individual or single household or, if used outside of a home, for use by the general public.

(9) "Disclose" means any action, set of actions, or omission in which a covered entity, data processer, or third party makes personal information available to another person, intentionally or unintentionally, including but not limited to sharing, publishing, releasing, transferring, disseminating, making available, selling, leasing, providing access to, failing to restrict access to, or otherwise communicating orally, in writing, electronically, or by any other means.

(10) "Harm" shall mean potential or realized adverse consequences to an individual or to society, including but not limited to:

(a) Direct or indirect financial harm;

(b) Physical harm or threats to individuals 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 an individual or class of individuals' 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 individuals' rights to due process or equal protection under the law;

(g) Loss of individual control over captured personal information via nonconsensual sharing of private information, data breach, or other actions that violate the rights listed in section 4 of this act;

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

(i) Other effects on an individual that may not be reasonably foreseeable to, contemplated by, or expected by the individual to whom the captured personal information relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered

entity that alter or limit that individual's choices or predetermines results.

(11) "Individual" means a natural person who is a Washington state resident. The location of a person in Washington state shall create a presumption that the person is a Washington state resident.

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

(13) "Personal information" means any information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other information to identify an individual, household, or device.

(14) "Processing" or "process" means any action or set of actions performed on or with personal information, including but not limited to collection, access, use, retention, sharing, monetizing, analysis, creation, generation, derivation, decision making, recording, alteration, organization, structuring, storage, disclosure, transmission, sale, licensing, disposal, destruction, deidentifying, or other handling of personal information; provided, however, that a person or entity that operates on captured personal information that is encrypted or otherwise in a format that makes it not accessible or susceptible to being made accessible to such person or entity in any comprehensible form shall not be deemed to be processing such captured personal information.

(15) "Proxy" or "proxies" means information that, by itself or in combination with other information, is used by a covered entity or Washington governmental entity in a way that discriminates based on actual or perceived personal characteristics or classes protected under Washington law.

(16) "Reasonably understandable" means a length and complexity that is easily understandable to the least sophisticated consumer.

(17) "Targeted advertisement" means an advertisement directed to an individual where the advertisement is selected based in whole or in part on personal information about the individual. It does not include advertisements directed to an individual based solely upon the individual's current visit to a website, application, service, or covered entity, or in direct response to the individual's request for information or feedback.

(18) "Third party" means, with respect to an individual's captured personal information, any person or entity that is not the covered entity or a data processer that obtained the individual's captured personal information from a covered entity or processor.

(19) "Use model" means a discrete purpose for which collected personal information is to be processed, including but not limited to first-party marketing, third-party marketing, first-party research and development, third-party research and development, and product improvement.

(20) "Washington governmental entity" shall mean 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. 4.** An individual residing in Washington state has the following rights with regard to the individual's personal information:

(1) The right to know what personal information a covered entity processes about the individual, including the categories and specific pieces of personal information the covered entity processes;

(2) The right to access and obtain the individual's personal information processed by a covered entity, in a machine-readable format that allows an individual to transfer their personal information from one entity to another entity without hindrance;

(3) The right to refuse consent for any processing of the individual's captured personal information that is not essential to the primary transaction;

(4) The right to correct inaccurate personal information;

(5) The right to require a covered entity and/or data processor to delete all captured personal information of the individual processed by the covered entity or data processor, provided that a covered entity that processes captured personal information from an

individual is required to not delete information to the extent it is exempt under section 9(1) of this act from the requirement of freely given, specific, informed, and unambiguous opt-in consent or to the extent it is required to be maintained by the covered entity under existing laws or regulations; and

(6) The right to not be subject to surreptitious surveillance.

NEW SECTION. **Sec. 5.** (1) Meaningful notice.

(a) A covered entity must make both a long-form privacy policy and a short-form privacy policy persistently and conspicuously available. Covered entities shall ensure that:

(i) Individuals interact with the short-form privacy policy upon the individual's first visit to the covered entity's website or use of the covered entity's mobile application;

(ii) In the case of in-person or noninternet electronic engagement, the short-form privacy policy is read to or otherwise presented to the individual prior to the time the covered entity first collects the individual's captured personal information;

(iii) The privacy policies are persistently available and readily accessible on the covered entity's website or mobile application;

(iv) The privacy policies are readily accessible at the primary physical place of business and any offline equivalent maintained by the covered entity; and

(v) The privacy policies are persistently and conspicuously available at or prior to the point of sale of a product or service, subscription to a service, or establishment of an account with the covered entity. If there is no such sale, subscription, or establishment, the privacy policies must be persistently and conspicuously available before the individual uses the product or service of the covered entity.

(b) The short-form privacy notice required under (a) of this subsection shall:

(i) Be clear, concise, well-organized, and complete;

(ii) Be clear and prominent in appearance;

(iii) Use clear and plain language;

(iv) Use visualizations where appropriate to make complex information understandable by the least sophisticated consumer;

(v) Be in English and any other language in which the covered entity communicates with the individual to whom the information pertains;

(vi) Be understandable by the least sophisticated consumer;

(vii) Be clearly distinguishable from other matters;

(viii) Not contain any unrelated, confusing, or contradictory information;

(ix) Be no more than 500 words, excluding the list of third parties with which the covered entity discloses captured personal information, as required under (c)(vi) of this subsection; and

(x) Be provided free of charge.

(c) The short-form privacy notice required under (a) of this subsection must include:

(i) What captured personal information is being processed;

(ii) The manner in which the captured personal information is processed;

(iii) How and for what purpose the covered entity processes the captured personal information;

(iv) How long the captured personal information will be retained;

(v) Whether and how the covered entity monetizes captured personal information;

(vi) To what types of third parties the covered entity discloses captured personal information and for what purposes; and

(vii) How the covered entity collects captured personal information, including offline practices, including but not limited to when the individual is not interacting directly with the covered entity.

(d) A by-entity list of the third parties referenced in (c)(vi) of this subsection must be provided either in the short-form privacy notice or in an easily accessible online form. If the policy is delivered verbally, the person communicating the policy must offer to read the list of third parties. If provided in the short-form privacy notice, such list must be offset by at least two line breaks from the rest of the short-form privacy notice required under (a) of this subsection.

(e) Within six months of enactment, the Washington state department of commerce shall establish a standardized short-form privacy notice that complies with this subsection (1).

(f) Within six months of enactment, the Washington state department of commerce shall determine whether a more concise presentation of a short-form privacy notice is appropriate where the policy is being communicated verbally, and if so, shall establish a

standardized short-form verbal privacy notice that complies with this subsection (1).

(g) To promote individuals' access to and awareness of the privacy notices, within six months of enactment, the Washington state department of commerce shall develop a recognizable and uniform logo or button to be used on covered entities' interaction pages linking to the entities' short-form privacy notice.

(h) The Washington state department of commerce may adopt regulations specifying additional requirements for the format and substance of short-form privacy notices.

(2) Opt-in consent.

(a) A covered entity shall not, without freely given, specific, informed, and unambiguous opt-in consent from an individual:

(i) Process the individual's captured personal information; or

(ii) Make any changes in the processing of the individual's captured personal information that would necessitate a change to the information required to be provided under subsection (1)(c) of this section.

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

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

(d) A covered entity shall provide a mechanism for an individual to withdraw previously given consent at any time. The individual shall be notified when the withdrawal of consent is complete. It must be as easy for an individual to withdraw their consent as it is for the individual to provide consent.

(e) Under no circumstances shall an individual's interaction with a covered entity's product or service when the covered entity has a terms of service or a privacy policy, including the short-form privacy notice, in and of itself constitute freely given, specific, informed, and unambiguous consent.

(f) To the extent that a covered entity must process internet protocol addresses, system configuration information, uniform resource locators of referring pages, locale and language preferences, keystrokes, and other captured personal information in

order to obtain individuals' freely given, specific, informed, and unambiguous opt-in consent, the covered entity shall:

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

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

(iii) Immediately delete the captured personal information if consent is not given.

(g) A covered entity shall not refuse to serve an individual who does not approve the processing of the individual's captured personal information under this section unless the processing is necessary for the primary purpose of the transaction that the individual has requested.

(h) A covered entity shall not discriminate against individuals by reason of their not granting opt-in consent to the processing of their personal information under this chapter or otherwise exercising their rights under this chapter, including but not limited to, by: Denying goods or services to the individual; 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 individual; and suggesting that the individual will receive a different price or rate for goods or services or a different level or quality of goods or services. Notwithstanding the above, a covered entity may, with the individual's opt-in consent given in compliance with this subsection (2), operate a program in which information, products or services sold to the individual are discounted based on that individual's prior purchases from the covered entity, provided that the captured personal information shall be processed solely for the purpose of operating such program.

(i) A covered entity 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 individual declines to give opt-in consent to captured personal information processing.

(j) The Washington state department of commerce is hereby authorized and directed to conduct a study to determine the most effective way for covered entities to obtain individuals' freely

given, specific, informed, and unambiguous opt-in consent for each type of captured personal information processing.

(k) The Washington state department of commerce may request data and information from covered entities conducting business in Washington state, other Washington state government entities administering notice and consent regimes, consumer protection experts, privacy advocates, and researchers, internet standards setting bodies such as the internet engineering taskforce and institute of electrical and electronics engineers, and other relevant sources to meet the purpose of the study.

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

(i) Covered entities must notify individuals of their rights under this chapter and obtain individuals' freely given, specific, informed, and unambiguous opt-in consent for each use model of captured personal information processing; and

(ii) Covered entities must notify individuals of their right to withdraw their consent at any time and how the right may be exercised.

(m) Within six months of enactment, the Washington state department of commerce shall adopt regulations grouping different types of processing of captured personal information by use model and permitting a covered entity to simultaneously obtain freely given, specific, informed, and unambiguous opt-in consent from an individual for multiple transactions of the same use model.

(3) Obligation of care.

(a) In storing, using, and transmitting captured personal information, a covered entity shall use practices that at least satisfy the reasonable standard of care within the covered entity's industry for protecting captured personal information from disclosure.

(b) The Washington state department of commerce, in consultation with the office of privacy and data protection, may develop appropriate security standards for captured personal information. This subsection preempts (a) of this subsection only to the extent that security standards developed are more protective of captured personal information than is the industry standard of care.

(4) Access to personal information.

(a) A covered entity that processes an individual's captured personal information must provide the individual with a reasonable

means to access their personal information processed by such entity, including:

(i) All personal information obtained about that individual from the individual or a third party, whether online or offline;

(ii) All information about where or from whom the covered entity obtained captured personal information; and

(iii) The types of third parties to which the covered entity has disclosed or will disclose captured personal information.

(b) A covered entity that processes an individual's captured personal information must provide the access to the individual's personal information under (a) of this subsection in a machine-readable and searchable format that allows the individual to transfer the personal information from one entity to another entity without hindrance.

(c) A covered entity that maintains an individual's captured personal information in a nonpublic profile or account must delete the captured personal information, and any information derived therefrom, pertaining to an individual upon that individual's request, provided that a covered entity that has collected captured personal information from an individual is not required to delete information to the extent it is exempt under section 9(1) of this act from the requirement of freely given, specific, informed, and unambiguous opt-in consent or is otherwise required by law or regulation to be retained by the covered entity.

(d) A covered entity must provide the opportunities required under this subsection (4) in a form that is:

(i) Clear and conspicuous;

(ii) Made available at no additional cost to the individual to whom the information pertains; and

(iii) In English and any other language in which the covered entity communicates with the individual to whom the information pertains.

(e) A covered entity must comply with an individual's request under this subsection (4) no later than 30 days after receiving a verifiable request from the individual.

(i) Where the covered entity has reasonable doubts or cannot verify the identity of the individual making a request under (b) through (d) of this subsection, the covered entity may request additional personal information necessary for the specific purpose of confirming the identity of the individual.

(ii) A covered entity may not deidentify an individual's captured personal information during the 60-day period beginning on the date the covered entity receives a request from the individual under (b) through (d) of this subsection.

(5) Correction and deletion of personal information.

(a) A covered entity that processes an individual's captured personal information shall provide the individual with a reasonable means to correct inaccurate or incomplete personal information processed by the covered entity.

(b) A covered entity that maintains an individual's captured personal information in a nonpublic profile or account must delete the captured personal information, and any information derived therefrom, pertaining to an individual upon that individual's request, provided that a covered entity that has collected captured personal information from an individual is required to not delete information to the extent it is exempt under section 9(1) of this act from the requirement of freely given, specific, informed, and unambiguous opt-in consent or is required by law or regulation to be retained by the covered entity.

(c) A covered entity must provide the opportunities required under this subsection (5) in a form that is:

(i) Clear and conspicuous;

(ii) Made available at no additional cost and with no transactional penalty to the individual to whom the information pertains; and

(iii) In English and any other language in which the covered entity communicates with the individual to whom the information pertains.

(d) A covered entity must comply with an individual's request under this subsection (5) no later than 30 days after receiving a verifiable request from the individual.

(i) Where the covered entity has reasonable doubts or cannot verify the identity of the individual making a request under (b) through (d) of this subsection, the covered entity may request additional captured personal information necessary for the specific purpose of confirming the identity of the individual.

(ii) A covered entity may not deidentify an individual's captured personal information while a request for correction or deletion is pending.

(6) Confidentiality and protection of data.

(a) A covered entity shall not disclose captured personal information to a third party unless that third party is contractually bound to the covered entity to meet the same privacy and security obligations as the covered entity.

(b) A covered entity shall exercise reasonable oversight and take reasonable actions, including auditing the data security and processing practices of third parties it provides captured personal information to at least once annually and ensure the third party's compliance with such contractual provisions. The covered entity shall publish the results of the audit publicly on its website.

(c) A covered entity shall not process captured personal information it has acquired from a third party, without the freely given, specific, informed, and unambiguous opt-in consent from the individual to whom that captured personal information pertains. If processing is necessary to obtain individuals' freely given, specific, informed, and unambiguous opt-in consent, the covered entity shall:

(i) Process only the captured personal information necessary to request freely given, specific, informed, and unambiguous opt-in consent; or

(ii) Immediately delete the captured personal information if consent is not given.

(d) If a covered entity that has facilitated access to captured personal information by other entities has knowledge that an entity to which captured personal information was provided is using such data in violation of this chapter, then the covered entity shall immediately limit the violator's access to such captured personal information and seek proof of destruction of such captured personal information by the violating entity.

(e) A covered entity shall not disclose captured personal information to a data processer unless the covered entity enters into a contractual agreement with the data processer that:

(i) Prohibits the data processer from processing the captured personal information for any purpose other than the purposes for which the individual provided the captured personal information to the covered entity;

(ii) Requires the data processer to meet the same privacy and security obligations as the covered entity; and

(iii) Prohibits the data processer from further disclosing or processing captured personal information it has acquired from the

covered entity except as explicitly authorized by the contract and consistent with this chapter.

(f) A covered entity shall exercise reasonable oversight and take reasonable actions, including auditing the data security and processing practices of the data processer at least once annually and ensure the data processor's compliance with such contractual provisions. The covered entity shall publish the results of the audit publicly on its website.

(7) Surreptitious surveillance.

A covered entity shall not activate the microphone, camera, or any other sensor on a device in the lawful possession of an individual that is capable of collecting or transmitting personal information, without providing the privacy notices required in subsection (1) of this section and obtaining the individual's freely given, specific, informed, and unambiguous opt-in consent pursuant to subsection (2) of this section 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 individual's freely given, specific, informed, and unambiguous opt-in consent pursuant to subsection (2) of this section.

NEW SECTION. **Sec. 6.** Age of responsibility.

(1) For the purposes of this chapter individuals ages 13 and older are deemed competent to exercise all rights granted to individuals under this chapter.

(2) Rights and obligations relating to individuals under the age of 13 shall be governed by the children's online privacy protection act (15 U.S.C. Sec. 6501 et seq.).

NEW SECTION. **Sec. 7.** In addition to all provisions of this chapter applicable to captured personal information, the following provisions shall be applicable to all biometric information, regardless of how such biometric information is processed.

(1) **Retention; disclosure; destruction.** A covered entity 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 individual's last interaction with the covered entity 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 covered entity or Washington governmental entity must be destroyed. Absent a valid warrant issued by a court of competent jurisdiction, a covered entity or Washington governmental entity in possession of biometric information must comply with its established retention schedule and destruction guidelines.

(2) **Processing.** No covered entity or Washington governmental entity may process an individual's biometric information, unless it first:

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

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

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

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

(3) **Disclosure.** No covered entity or Washington governmental entity in possession of biometric information may disclose or otherwise disseminate an individual's biometric information unless:

(a) The individual 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 9(2)(b)(i) of this act has allowed at least 10 business days for the subject to seek review of or otherwise challenge the subpoena.

(4) **Monetizing.** No covered entity or Washington governmental entity in possession of biometric information may monetize, or otherwise profit from an individual's biometric information; provided only that a covered entity may process an individual's biometric information, with full disclosure and opt-in consent consistent with section 5(2) of this act, in a service in which the covered entity reports to the individual the biometric information processed and/or utilizes the biometric information to design or recommend actions or products that have been specifically requested by the individual 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 covered entity or governmental entity may list personal information such as name or birthdate and biometric information such as height, weight, or photograph on an issued license, membership or identification card for the sole purpose of allowing an employee or other representative of the covered 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 individual 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 covered entity 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.

NEW SECTION. **Sec. 8.** (1) It shall be an unlawful discriminatory practice:

(a) For a covered entity or Washington governmental entity to process captured personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment,

finance, health care, credit, insurance, housing, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of an individual's or class of individuals' actual, perceived, or proxies for actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, except as specifically authorized by law;

(b) For a covered entity or Washington governmental entity to process captured personal information in a manner that discriminates in or otherwise makes unavailable, whether in a commercial transaction or otherwise, any place of public resort, accommodation, assemblage, or amusement as defined in RCW 49.60.040, on the basis of an individual's or class of individuals' actual, perceived, or proxies for actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, except as specifically authorized by law;

(c) For a covered entity or Washington governmental entity that uses captured personal information in sales or placement of targeted advertisements in which persons or entities offer commercial transactions in employment, finance, health care, credit, insurance, housing, or education opportunities, to target such advertisements on actual, perceived, or proxies for actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, except as specifically authorized by law.

(d) For a covered entity or Washington governmental entity to operate, install, or commission the operation or installation of equipment incorporating face recognition in any place of public resort, accommodation, assemblage, or amusement, as defined in RCW 49.60.040. For the purpose of this subsection, "face recognition" means: (i) An automated or semiautomated process by which an individual is identified or attempted to be identified based on the characteristics of the individual's face; or (ii) an automated or semiautomated process by which the characteristics of an individual's face are analyzed to determine the individual's sentiment, state of mind, or other propensities including, but not limited to, the person's level of dangerousness;

(e) For a covered entity or Washington governmental entity to operate, install, or commission the operation or installation of equipment incorporating artificial intelligence-enabled profiling in any place of public resort, accommodation, assemblage, or amusement, as defined in RCW 49.60.040, or to use artificial intelligence-enabled profiling to make decisions that produce legal effects or similarly significant effects concerning individuals. Decisions that include legal effects or similarly significant effects concerning consumers include, without limitation, denial or degradation of consequential services or support, such as financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water. For the purposes of this subsection, "artificial intelligence-enabled profiling" means the automated or semiautomated process by which the external or internal characteristics of an individual are analyzed to determine, infer, or characterize an individual's state of mind, character, propensities, protected class status, political affiliation, religious beliefs or religious affiliation, immigration status, or employability.

(2) A covered entity or Washington governmental entity that sells or places targeted advertisements for employment, finance, health care, credit, insurance, housing, or education opportunities shall require persons or entities on whose behalf such sales or placement is made to certify that they are in compliance with RCW 49.60.030.

(3) Nothing in this section shall limit covered entities or Washington governmental entities from processing captured personal information for legitimate testing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of the covered entity's or Washington governmental entity's compliance with this section.

NEW SECTION. **Sec. 9.** (1) With respect to captured personal information that is not biometric information, a covered entity shall not be required to obtain freely given, specific, informed, and unambiguous opt-in consent from an individual under section 5(2) of this act if the processing is necessary to execute the specific transaction for which the individual is providing captured personal information, such as the provision of financial information to complete a purchase or the provision of a mailing address to deliver

a package. However, captured personal information 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 individual to whom the captured personal information pertains, except as required by law.

(2) With respect to captured personal information generally, a covered entity or Washington governmental entity shall not be required to obtain freely given, specific, informed, and unambiguous opt-in consent from an individual under section 5(2) or 7(1) of this act if:

(a) It believes that an emergency involving immediate danger of death or serious physical injury to any individual requires obtaining without delay captured personal information 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 an individual requires obtaining without delay captured personal information relating to the emergency; and

(ii) Simultaneous with the covered entity or Washington governmental entity obtaining captured personal information under this subsection (a), the covered entity or Washington governmental entity shall use reasonable efforts to inform the individual of the captured personal information obtained; the details of the emergency; and the reasons why the covered entity 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 captured personal information, serve or deliver the following information to the subject of 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 individual of the nature of the inquiry with reasonable specificity;

(B) That captured personal information maintained for the individual 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 captured personal information requested or supplied; and

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

(ii) A covered entity 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 an individual, 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 covered entity subject to a subpoena shall postpone compliance therewith until it has given the subject of the subpoena notice of the information required under this subsection (2)(b)(i) 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;

(d) Processing involves only deidentified information.

(3) This chapter shall not apply to captured personal information 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 an individual is a covered entity's placement of that individual's personal information in the public domain, such as recording of a real estate deed showing

name and address, the covered entity shall have the same rights as any other person or entity with regard to such information.

(5) This chapter shall not apply to individuals sharing their personal contact information such as email addresses with other individuals in workplace, social, political or similar settings where the purpose of the information is to facilitate communication among such individuals, provided that any processing of such contact information beyond interpersonal communication shall be covered by this chapter. This chapter shall not apply to entities' publication of entity-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 entity's operations.

(6) Nothing in this chapter shall diminish any individual's or entity's rights or obligations under chapter 70.02 RCW.

NEW SECTION. **Sec. 10.** Data protection assessments.

(1) Covered entities must conduct and document a data protection assessment of each of the following processing activities involving captured personal information:

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

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

(c) The processing of captured personal information for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(i) Unfair or deceptive treatment of, or disparate impact on, individuals;

(ii) Financial, physical, or reputational injury to individuals;

(iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of individuals, where such intrusion would be offensive to a reasonable person; or

(iv) Other substantial injury to individuals; and

(d) Any processing activities involving captured personal information that present a heightened risk of harm to individuals.

Such data protection assessments must take into account the type of captured personal information to be processed by the covered entity and the context in which the captured personal information is 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 covered entity, individual, other stakeholders, and the public against the potential risks to the rights of the individual associated with such processing, as mitigated by safeguards that can be employed by the covered entity to reduce such risks. The use of deidentified data and the reasonable expectations of individuals, as well as the context of the processing and the relationship between the covered entity and the individual whose personal data will be processed, must be factored into a data protection assessment by the covered entity.

(3) The attorney general may request, in writing, that a covered entity disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The covered entity must make a data protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data protection assessment for compliance with the responsibilities contained in this chapter 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 covered entity 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. 11.** (1) Private right of action.

(a) The legislature finds that the practices of covered entities regulated 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 competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

(b) An individual 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 or to waive the right to bring an action on behalf of a class similarly situated.

(c) A violation of this chapter or a regulation adopted under this chapter with respect to the captured personal information of an individual constitute a rebuttable presumption of harm to that individual.

(d) In a private civil action against a covered entity in which the plaintiff prevails, the court shall award the greater of liquidated damages of $2,000 per violation or actual damages, provided that the court may, in its discretion, increase the damages awarded up to an amount not to exceed three times the actual damages. The court may also award any other relief including, but not limited to, injunctive or declaratory relief, that the court determines appropriate.

(e) In a private civil action against a Washington governmental entity under this chapter in which the plaintiff prevails, the court shall award the greater of liquidated damages of $2,000 per violation or actual damages. The court may also award any other relief including, but not limited to, injunctive or declaratory relief, that the court determines appropriate.

(f) In an action brought by the attorney general, the court may award:

(i) Injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with this chapter;

(ii) Civil penalties of up to $25,000 per violation or up to four percent of annual revenue, whichever is greater, of the covered entity, data processor, or third party;

(iii) Other appropriate relief, including restitution, to redress harms to individuals or to mitigate all substantial risk of harm; and

(iv) Any other relief the court determines appropriate.

(g) In addition to any relief awarded pursuant to (d) through (f) of this subsection, the court shall award reasonable attorneys' fees and costs to any prevailing plaintiff.

(2) When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the precautions taken to prevent a violation.

(3) Each individual whose captured personal information was unlawfully processed, each instance of processing counts as a separate violation. Each provision of this chapter that was violated counts as a separate violation.

(4) It is a violation of this chapter for a covered entity, Washington governmental entity, or anyone else acting on behalf of a covered entity or Washington governmental entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this chapter. An individual who is injured by a violation of this subsection (4) may bring a civil action for monetary damages and injunctive relief in any court of competent jurisdiction.

(5) If a series of steps or transactions with regard to a set of personal information are undertaken with the intention of avoiding the intent of this chapter, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this chapter.

(6) Any provision of a contract or agreement of any kind, including a covered entity's terms of service or a privacy policy, including the short-form privacy notice required under section 5(1) of this act, that purports to waive or limit in any way an individual's rights under this chapter, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.

(7) For purposes of causes of action based on violations of this chapter, the statute of limitations period shall commence only upon discovery of the violation of this chapter or of the injury caused by such a violation, whichever occurs later.

(8) A covered entity that is a provider of an interactive computer service, as defined in 47 U.S.C. Sec. 230, may not be treated as the publisher or speaker of any personal information provided by another information content provider, as defined in 47 U.S.C. Sec. 230. Allowing the posting of information by a user without other action by the interactive computer service is not considered processing of the personal information by the interactive computer service.

(9) No private or government action brought pursuant to this chapter shall preclude any other action under this chapter.

(10) This section does not apply to any violations that occurred prior to the effective date of this section.

NEW SECTION. **Sec. 12.** (1) This chapter shall not supersede local or state laws, regulations, or ordinances except to the extent that it provides stronger privacy protections for individuals.

(2) Subject to subsection (3) of this section, covered entities that are subject to federal laws concerning the processing of individuals' captured personal information are covered by this chapter to the extent that it provides stronger privacy protections for individuals than those federal laws and that those federal laws do not preempt state laws.

(3) This chapter shall not override any valid law or regulation explicitly compelling disclosure of or giving access to captured personal information such as in chapter 42.17A RCW.

NEW SECTION. **Sec. 13.** 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. 14.** A new section is added to chapter 42.56 RCW to read as follows:

Data protection assessments submitted by a covered entity to the attorney general in accordance with the requirements under section 10 of this act are exempt from disclosure under this chapter.

NEW SECTION. **Sec. 15.** Sections 1 through 12 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 16.** Section 11 of this act takes effect July 1, 2024.

NEW SECTION. **Sec. 17.** This chapter does not apply to nonprofit corporations until July 31, 2025.

--- END ---