S-3347.3

SENATE BILL 5813

State of Washington 67th Legislature 2022 Regular Session

By Senators Carlyle and Nguyen

AN ACT Relating to establishing data privacy protections to strengthen a consumer's ability to access, manage, and protect their personal data; adding a new section to chapter 42.56 RCW; adding new chapters 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.** 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) Washington is a technology leader on a national and global level and recognizes its distinctive position in promoting the efficient balance of consumer privacy and economic benefits. 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) From a very young age, today's youth spend an extensive amount of their time engaged in online activities and services for various purposes including education, socializing, shopping, gaming, and entertainment. Children and adolescents navigate various websites and online applications without fully understanding what personal data is being collected about them, how this data can impact them in the future, or how to ensure the privacy and security of their personal data. The personal data of this vulnerable population requires and deserves additional protections, which includes parental or guardian oversight, adolescent control of data, and the ability for adults to delete their personal data from when they were a child or adolescent.

(4) There are many different types of businesses that collect data about and from consumers. However, a data broker is in the business of combining and selling data about consumers with whom it does not have a direct relationship. Data brokers often collect data from multiple sources, all while consumers may not know that the data broker exists. While data brokers offer many benefits in a modern economy, such as providing information that is critical to services including credit reporting, background checks, risk mitigation, fraud detection, and people search, there are also risks associated with the prevalent combination and sale of data about consumers. These risks may relate to a consumer's ability to know and control information held and sold about them and risks due to the unauthorized or harmful acquisition and use of consumer information.

(5) In order to provide consumers with more control over how their personal data is used by businesses, several states have enacted laws that provide consumers with the right to opt out of targeted advertising and the sale of their data. In an effort to make the opt out right more workable for consumers, such laws often authorize consumers to request to opt out through do not track mechanisms and require businesses to recognize these requests. However, technical specifications needed to implement such a

requirement are in the early stages of development and it is worth taking a measured, thoughtful approach.

(6) With this act, the legislature intends to: Strengthen and expand existing privacy protections for Washington residents by establishing additional protections and controls for the personal data of children and adolescents; provide consumers transparency about data brokers; require data brokers to allow consumers to access, delete, and correct their data; and engage in deliberate, inclusive rule making to determine appropriate and reasonable technical specifications for honoring consumer requests to opt out of certain processing. In addition, this act imposes affirmative obligations upon companies to safeguard personal data and provide clear, understandable, and transparent information to consumers about how their personal data is used.

PART 1
DATA RELATED TO CHILDREN AND ADOLESCENTS

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

(1) "Adolescent" means a natural person who is at least 13 years old and younger than 18 years old and a Washington resident.

(2) "Adult" means a natural person who is 18 years old or older and a Washington resident.

(3)(a) "Biometric data" means any personal data generated from the measurement or specific technological processing of a child's or an adolescent's biological, physical, or physiological characteristics, which allows or confirms the unique identification of that child or adolescent, including fingerprints, voice prints, iris or retina scans, facial scans or templates, genetic data, and gait.

(b) "Biometric data" does not include writing samples, written signatures, photographs, voice recordings, videos, demographic data, or physical characteristics such as height, weight, hair color, or eye color, provided that such information is not used for the purpose of identifying a child's or an adolescent's unique biological, physical, or physiological characteristics.

(4) "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects personal data of a child or an adolescent, or on the behalf of which such data is collected, and that alone, or jointly with others, determines the purposes and means of the processing of personal data of a child or an adolescent.

(5) "Child" means a natural person who is younger than 13 years old and a Washington resident.

(6) "Consent" means any freely given, specific, informed, and unambiguous indication of wishes of an adolescent or a parent or legal guardian of a child by which the adolescent or the parent or legal guardian of a child signifies agreement to the processing of personal data relating to the child or the adolescent 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.

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

(8) "Deidentified data" means data that cannot reasonably be used to infer information about, associate with, or otherwise link to a natural person, household, or a device linked to such a person or household, provided that the business that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be used to infer information about, associate with, or otherwise link to, a natural person, household, or a device linked to such a person or household; (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 data to comply with all provisions of this subsection.

(9)(a) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material.

(b) For the purposes of this subsection "genetic material" includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from the analysis of the biological sample, and any information extrapolated, derived, or inferred therefrom.

(10) "Individual" means a natural person who is an adolescent, an adult, or a parent or legal guardian of a child.

(11) "Known adolescent" means an adolescent under circumstances where a business has actual knowledge of, or willfully disregards, the adolescent's age.

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

(13)(a) "Personal data" means data that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular child or adolescent.

(b) "Personal data" includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular child or adolescent:

(i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, telephone number, insurance policy number, bank account number, credit card number, debit card number, or other similar identifiers;

(ii) Characteristics of protected classifications under Washington or federal law, as they may be construed or amended from time to time;

(iii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(iv) Biometric data;

(v) Internet or other electronic network activity information including, but not limited to, browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement;

(vi) Specific geolocation data;

(vii) Audio, electronic, visual, thermal, olfactory, or similar information;

(viii) Education information, defined as information that is not publicly available personally identifiable information as defined in the family educational rights and privacy act (20 U.S.C. Sec. 1232g, 34 C.F.R. Part 99);

(ix) Inferences drawn from any of the information identified in this subsection to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; or

(x) Sensitive data.

(c) "Personal data" does not include deidentified information.

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

(15)(a) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning a child's or an adolescent's economic situation, health, personal preferences, interests, character, reliability, behavior, social or political views, physical location, movements, or demographic characteristics, including race, gender, or sexual orientation.

(b) "Profiling" does not include evaluation, analysis, or prediction based solely upon a child's or an adolescent's current activity, including a child's or an adolescent's current search query or current visit to a website or online application, if no personal data is retained after the completion of the activity for the purposes identified in (a) of this subsection.

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

(b) "Publicly available information" does not include: (i) Information derived from publicly available information; (ii) biometric data; or (iii) nonpublicly available information that has been combined with publicly available information.

(17)(a) "Sell," "selling," "sale," or "sold" means selling, renting, licensing, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal data of a child or an adolescent by the business to a third party for monetary or other valuable consideration.

(b) For the purposes of this chapter, a business does not sell personal data when: (i) An adolescent or a parent or legal guardian of a child provides consent to the business directing the business to: (A) Intentionally disclose personal data; or (B) intentionally interact with one or more third parties; (ii) the business discloses personal data to a service provider who processes the data on behalf of the business; or (iii) the business transfers to a third party the personal data of a child or an adolescent 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 business, provided that personal data is used or shared consistently with this chapter. If a third party materially alters how it uses or shares the personal data of a child or an adolescent in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the individual. The notice must be sufficiently prominent and robust to ensure that existing individuals can easily exercise their choices consistently with this chapter. This subsection does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Washington consumer protection act, chapter 19.86 RCW.

(18)(a) "Sensitive data" means personal data that reveals: (i) The social security, driver's license, state identification card, or passport number of a child or an adolescent; (ii) a child's or an adolescent's account log-in, financial account, debit card, or credit card number, in combination with any required security or access code, password, or credentials allowing access to an account; (iii) specific geolocation data of a child or an adolescent; (iv) the racial or ethnic origin, religious or philosophical beliefs, or union membership a child or an adolescent; (v) the contents of a child's or an adolescent's mail, email, and text messages, unless the business is the intended recipient of the communication; (vi) biometric data of a child or an adolescent; and (vii)(A) any information that describes or reveals the past, present, or future physical health,

mental health, disability, or diagnosis of a child or an adolescent; or (B) personal data collected and analyzed concerning the sexual orientation of a child or an adolescent.

(b) Sensitive data that is "publicly available information" pursuant to subsection (16) of this section is not considered sensitive data or personal data.

(19) "Service provider" means a natural or legal person who processes personal data of a child or an adolescent on behalf of a business pursuant to a binding contract that: (a) Sets out the processing instructions to which the service provider is bound; and (b) prohibits the service provider from: (i) Processing the personal data for any purpose outside of the instructions in the contract; or (ii) determining the purposes and means of the processing of the personal data. A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under this chapter, is deemed a service provider for purposes of this chapter.

(20) "Specific geolocation data" means data derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms that directly identifies the past or present physical location of a child or an adolescent or a device 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 information excludes the content of communications.

(21) "Targeted advertising" means advertising based upon profiling.

(22) "Third party" means a natural or legal person, public authority, agency, or body other than the business, service provider, adolescent, adult, child, or a parent or legal guardian of the child.

NEW SECTION. **Sec. 102.** (1) A business may not process the personal data or sensitive data of a known child without obtaining consent from the child's parent or legal guardian.

(2) A business may not process the personal data or sensitive data of a known adolescent without obtaining separate and express consent from the adolescent.

(3) A business may not process the personal data of a known adolescent for purposes of targeted advertising or the sale of

personal data without obtaining separate and express consent from the adolescent.

(4) Businesses that obtain verifiable parental consent to process personal data of a child in compliance with the children's online privacy protection act, Title 15 U.S.C. Secs. 6501 through 6506 and its implementing regulations, are deemed compliant with any obligation to obtain consent from a child's parent or legal guardian under this chapter.

NEW SECTION. **Sec. 103.** (1) The parent or legal guardian of a child has the right to confirm whether a business is processing the child's personal data and to access any such personal data.

(2) The parent or legal guardian of a child has the right to correct inaccurate personal data concerning the child, taking into account the nature of the personal data and the purposes of the processing of the personal data.

(3) The parent or legal guardian of a child has the right to delete personal data concerning the child.

NEW SECTION. **Sec. 104.** (1) An adolescent has the right to confirm whether a business is processing the adolescent's personal data and to access any such personal data.

(2) An adolescent has the right to correct inaccurate personal data concerning the adolescent, taking into account the nature of the personal data and the purposes of the processing of the personal data.

(3) An adolescent has the right to delete personal data concerning the adolescent.

NEW SECTION. **Sec. 105.** (1) An adult has the right to confirm whether a business processed or is processing personal data pertaining to the adult as a child or an adolescent and to access any such personal data.

(2) An adult has the right to correct inaccurate personal data pertaining to the adult as a child or an adolescent, taking into account the nature of the personal data and the purposes of the processing of the personal data.

(3) An adult has the right to delete personal data pertaining to the adult as a child or an adolescent.

NEW SECTION. **Sec. 106.** (1) Businesses must provide one or more secure and reliable means by which requests to exercise the rights described in sections 103 through 105 of this act may be accomplished. These means must take into account the ways in which individuals interact with the business and the need for secure and reliable communication of the requests.

(2) Businesses may not require individuals to create a new account in order to exercise a right described in sections 103 through 105 of this act, but may require an individual to use an existing account to exercise the rights.

(3) A business must comply with a request to exercise the rights in sections 103 through 105 of this act as soon as feasibly possible, but no later than 30 days after receipt of the request. That period may be extended once by an additional 30 days where reasonably necessary, taking into account the complexity and number of the requests. The business must inform the individual submitting the request of such an extension within 30 days of receipt of the request, together with the reasons for the delay.

(4) Businesses may not charge a fee for responding to requests to exercise the rights in sections 103 through 105 of this act unless the requests made by an individual are manifestly unfounded or excessive, in particular because of their repetitive character, in which case the business may either: (a) Charge a reasonable fee to cover the administrative costs of complying with the request; or (b) refuse to act on the request. The business bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(5) A business is not required to comply with a request to exercise any of the rights under sections 103 through 105 of this act if the business is unable to authenticate the request using commercially reasonable efforts. In such a case, the business may request the provision of additional information reasonably necessary to authenticate the request.

(6) Any provision of a contract or agreement of any kind that purports to waive or limit in any way the rights of a child, a parent or legal guardian, an adolescent, or an adult under this chapter is deemed contrary to public policy and is void and unenforceable.

NEW SECTION. **Sec. 107.** (1) A business may not process the personal data of a known adolescent or a known child in any way that:

(i) Unfairly disadvantages the adolescent or the child considering the benefits of the processing, the risk of harm to the adolescent or the child, and the ability of the business to avoid any potential harm or detriment to the adolescent or the child; (ii) results in reasonably foreseeable harm to a known adolescent or known child; or (iii) would be unexpected and highly offensive to a reasonable person.

(2) A business shall provide a publicly available, reasonably accessible, clear, and meaningful privacy notice that includes:

(a) The categories of personal data relating to children or adolescents that are processed by the business;

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

(c) A clear, conspicuous, and prominent description of how and where the rights contained in sections 103 through 105 of this act may be exercised;

(d) The categories of personal data pertaining to children or adolescents that the business shares with third parties, if any; and

(e) The categories of third parties, if any, with whom the business shares personal data pertaining to children or adolescents.

(3) A business shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data pertaining to children and adolescents. The data security practices must be appropriate to the volume and nature of the personal data at issue.

(4) A business's collection of a child's or adolescent's personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which data is processed.

(5) Except as provided in this chapter, a business may not process the personal data of a child or an adolescent for purposes that are not reasonably necessary to, or compatible with, the specified purposes for which the personal data is processed unless the business obtains the necessary consents as described in section 102 of this act.

(6) A business may not retain personal data of a child or adolescent for longer than is necessary to fulfill a transaction or provide a service requested by the child or adolescent or such other purposes as permitted by this chapter. The business must implement a

reasonable and appropriate data disposal policy based on the nature and sensitivity of the personal data.

(7) The personal data of a child or adolescent may not be used to direct content to the child or adolescent, or a group of individuals similar to the child or adolescent, on the basis of race, socioeconomic factors, or any proxy thereof.

(8) A business may not disclose the personal data of a known adolescent or known child with any third party except as consistent with the obligations and rights contained in this chapter.

(9) A business may not engage in abusive trade practices concerning the processing of the personal data of a known adolescent or a known child, meaning practices that: (a) Materially interfere with the ability of adolescents, children, parents, or lawful guardians to understand a term or condition of a product or service involving the processing of personal data; or (b) unreasonably take advantage of or unreasonably fail to account for or remedy: (i) A lack of understanding by an adolescent, a child, or a parent or lawful guardian of the material risks, costs, or conditions of a product or service involving the processing of personal data; (ii) the inability of an adolescent, a child, or a parent or lawful guardian to protect the interests of the adolescent, child, or parent or lawful guardian in selecting or using a product or service involving the processing of personal data; or (iii) the reasonable reliance by an adolescent, a child, or a parent or lawful guardian on a business to act in the best interests of the adolescent or child.

(10) A business may not discriminate against a child, a parent or legal guardian of a child, an adolescent, or an adult for exercising any of the rights contained in this chapter, including denying them goods or services, charging different prices or rates for goods or services, and providing a different level of quality of goods and services. This subsection does not prohibit a business from offering a different price, rate, level, quality, or selection of goods or services to a parent or legal guardian of a child or an adolescent, including offering goods or services for no fee, if: (a) The offering is in connection with voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; (b) the use and any dissemination of personal data as part of the program is clearly and conspicuously disclosed, separate and apart from any other terms applicable to the program, to the parent or legal guardian of a child or the adolescent; (c) the parent or legal

guardian of a child or the adolescent provides consent to such use and disclosures; and (d) any third party who receives personal data as part of the program uses the personal data only for purposes of facilitating the benefits to which the parent or legal guardian of a child or the adolescent is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

NEW SECTION. **Sec. 108.** (1) A business must conduct and document a data protection assessment of each of its processing activities involving the personal data of children or adolescents. Such a data protection assessment must take into account the type of personal data to be processed by the business, including the extent to which the personal data is sensitive data, and the context in which the personal data is to be processed.

(2) A data protection assessment conducted under subsection (1) of this section must identify and weigh the benefits that may flow directly and indirectly from the processing to the business, the adolescent or child, other stakeholders, and the public against the potential risks to the rights of the adolescent, child, or parent or legal guardian of the child associated with such processing, as mitigated by safeguards that can be employed by the business to reduce such risks. The use of deidentified data and the reasonable expectations of adolescents, children, and parents or legal guardians, as well as the context of the processing and the relationship between the business and the adolescent, child, or parent or legal guardian must be factored into this assessment by the business.

(3) The attorney general may request, in writing, that a business disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The business 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 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) A data protection assessment conducted by a business for the purpose of compliance with other laws or regulations may qualify under this section if it has a similar scope and effect.

NEW SECTION. **Sec. 109.** (1) The obligations imposed on businesses or service providers under this chapter do not restrict a business's or service provider's ability to:

(a) Comply with federal, state, or local law; or

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

(2) A business is not required to comply with a request to delete personal information pursuant to sections 103(3), 104(3) or 105 of this act if it is necessary for the business to maintain the personal data to:

(a) Cooperate with law enforcement agencies concerning conduct or activity that the business or service provider reasonably and in good faith believes may violate federal, state, or local law;

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

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

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

(e) Perform solely internal operations that are reasonably aligned or compatible with the expectations of the parent or legal guardian of a child or the adolescent, as applicable, based upon the existing relationship that the business has with the parent or legal guardian of a child or the adolescent.

(3) The obligation to delete personal data pursuant to sections 103(3), 104(3) or 105 of this act does not apply to publicly available information.

(4) Obligations imposed on a business under this chapter may not 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.

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

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

(7) Personal data that is processed by a business pursuant to this section may be processed solely to the extent that the processing is: (a) Necessary, reasonable, and proportionate to the purposes listed in this section; (b) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section; and (c) insofar as possible, taking into account the nature and purpose of processing the personal data, subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal information, and to reduce reasonably foreseeable risks of harm to individuals.

NEW SECTION. **Sec. 110.** (1) Except as provided in subsection (2) of this section, nothing in this chapter creates an independent cause of action, except for the actions brought by the attorney general to enforce this chapter. Except as provided in subsection (2) of this section, no person, except for the attorney general, may enforce the rights and protections created by this chapter in any action. However, nothing in this chapter limits any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than this chapter, the person continues to have those rights and protections notwithstanding the existence of this chapter.

(2) An adolescent, an adult, or a parent or legal guardian of a child alleging a violation of sections 103, 104, and 105 of this act may bring a civil action in any court of competent jurisdiction. Remedies are limited to appropriate injunctive relief necessary and

proportionate to remedy the violation against the aggrieved adolescent, adult, or child. The court shall also award reasonable attorneys' fees and costs directly incurred in pursuit of claims under this chapter to any prevailing plaintiff.

NEW SECTION. **Sec. 111.** (1) Except as provided in section 110 of this act, this chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

(2) 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.

(3) The legislative declarations in this section do not apply to any claim or action by any party other than the attorney general alleging that conduct regulated by this chapter violates chapter 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

(4) In the event of a business's or service provider's violation under this chapter, prior to filing a complaint, the attorney general must provide the business or service provider 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 business or service provider has failed to cure any alleged violation, the attorney general may bring an action against the controller or processor as provided under this chapter.

(5) In determining a civil penalty under this chapter, the court must consider, as mitigating factors, a business's or service provider'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.

(6) All receipts from the imposition of civil penalties under this chapter must be deposited into the consumer privacy account created in section 112 of this act.

NEW SECTION. **Sec. 112.** 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. 113.** A new section is added to chapter 42.56 RCW to read as follows:

A data protection assessment submitted by a business to the attorney general in accordance with the requirements under section 108 of this act is exempt from disclosure under this chapter.

PART 2
DATA BROKERS

NEW SECTION. **Sec. 201.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1)(a) "Biometric data" means any personal data generated from the measurement or specific technological processing of a consumer's biological, physical, or physiological characteristics, which allows or confirms the unique identification of that consumer, including fingerprints, voice prints, iris or retina scans, facial scans or templates, genetic data, and gait.

(b) "Biometric data" does not include writing samples, written signatures, photographs, voice recordings, videos, demographic data, or physical characteristics such as height, weight, hair color, or eye color, provided that such information is not used for the purpose of identifying a consumer's unique biological, physical, or physiological characteristics.

(2)(a) "Brokered personal data" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) Name;

(ii) Address;

(iii) Date of birth;

(iv) Place of birth;

(v) Mother's maiden name;

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii) Name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) Other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(b) "Brokered personal data" does not include publicly available information to the extent that it is related to a consumer's business or profession.

(3) "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal data, or on the behalf of which such data is collected, and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal data.

(4) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal data pertaining to a consumer by any means. This includes receiving data from the consumer, either actively or passively, or by observing the consumer's behavior.

(5) "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.

(6) "Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does

not include a natural person acting in a commercial or employment context.

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

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

(ii) For the purposes of this subsection, examples of a "direct relationship" with a business include if the consumer is a past or present: (A) Customer, client, subscriber, user, or registered user of the business's goods or services; (B) employee, contractor, or agent of the business; (C) investor in the business; or (D) donor to the business.

(b)(i) "Data broker" does not include the following activities conducted by a business, and the collection and sale or licensing of brokered personal data incidental to conducting these activities: (A) Developing or maintaining third-party e-commerce or application platforms; (B) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (C) providing publicly available information related to a consumer's business or profession; or (D) providing publicly available information via real-time or near real-time alert services for health or safety purposes.

(ii) For the purposes of this subsection (8)(b), the phrase "sale or licensing" does not include a: (A) One-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or (B) sale or licensing of information that is merely incidental to the business.

(9) "Deidentified data" means information that cannot reasonably be used to infer information about, associate with, or otherwise link to, a natural person, household, or a device linked to such a person or household, provided that the business that possesses the information: (a) Takes reasonable measures to ensure that the information cannot be used to infer information about, associate with, or otherwise link to, a natural person, household, or a device linked to such a person or household; (b) publicly commits to

maintain and use the information only in a deidentified fashion and not attempt to reidentify the information; and (c) contractually obligates any recipients of the information to comply with all provisions of this subsection.

(10)(a) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material.

(b) For the purposes of this subsection, "genetic material" includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from the analysis of the biological sample, and any information extrapolated, derived, or inferred therefrom.

(11) "Person" means any natural person, firm, partnership, corporation, association, union, or other organization capable of suing or being sued in a court of law.

(12)(a) "Personal data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

(b) "Personal data" includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, telephone number, insurance policy number, bank account number, credit card number, debit card number, or other similar identifiers;

(ii) Characteristics of protected classifications under Washington state or federal law, as they may be construed or amended from time to time;

(iii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(iv) Biometric data;

(v) Internet or other electronic network activity information including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;

(vi) Specific geolocation data;

(vii) Audio, electronic, visual, thermal, olfactory, or similar information;

(viii) Education information, defined as information that is not publicly available personally identifiable information as defined in the family educational rights and privacy act (20 U.S.C. Sec. 1232g, 34 C.F.R. Part 99);

(ix) Inferences drawn from any of the information identified in this subsection to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; or

(x) Sensitive data.

(c) "Personal data" does not include deidentified data.

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

(14) "Processor" means a natural or legal person who processes personal data on behalf of a business pursuant to a binding contract that: (a) Sets out the processing instructions to which the processor is bound; and (b) prohibits the processor from: (i) Processing the personal data for any purpose outside of the instructions in the contract; or (ii) determining the purposes and means of the processing of the personal data.

(15) "Profiling" means any form of automated processing of personal information to evaluate, analyze, or predict personal aspects concerning a consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(16)(a) "Publicly available information" means information that: (i) Is lawfully made available from federal, state, or local government records; (ii) a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or (iii) is directly and voluntarily

disclosed to the general public by the consumer to whom the information relates.

(b) "Publicly available information" does not mean: (i) Information derived from publicly available information; (ii) biometric data; or (iii) nonpublicly available information that has been combined with publicly available information.

(17)(a) "Sell," "selling," "sale," or "sold" means selling, renting, licensing, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal data by a business to a third party for monetary or other valuable consideration.

(b) For purposes of this chapter, a business does not sell personal data when: (i) A consumer provides consent to the business directing the business to: (A) Intentionally disclose personal data; or (B) intentionally interact with one or more third parties; (ii) it discloses personal data to a processor who processes the data on behalf of the business; or (iii) the business transfers to a third party the personal data of a consumer 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 business, provided that data is used or shared consistently with this chapter. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this chapter. This subsection does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Washington consumer protection act, chapter 19.86 RCW.

(18)(a) "Sensitive data" means personal data that reveals: (i) A consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's account log-in, financial account, debit card, or credit card number, in combination with any required security or access code, password, or credentials allowing access to an account; (iii) specific geolocation data; (iv) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (v) the contents of a consumer's mail,

email, and text messages, unless the business is the intended recipient of the communication; (vi) a consumer's biometric data; and (vii)(A) any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis of a consumer; or (B) personal data collected and analyzed concerning a consumer's sexual orientation.

(b) Sensitive data that is "publicly available information" pursuant to subsection (16) of this section is not considered sensitive data or personal data.

(19) "Specific geolocation data" means data derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms that directly identifies the past or present physical location of a natural person or a device 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.

(20) "Third party" means a natural or legal person, public authority, agency, or body other than the business, consumer, or processor.

NEW SECTION. **Sec. 202.** (1) On or before January 31st following each year in which a business meets the definition of a data broker, the business shall register with the secretary of state pursuant to the requirements of this section.

(2) In registering with the secretary of state pursuant to subsection (1) of this section, a data broker shall:

(a) Pay a registration fee in an amount determined by the secretary of state, not to exceed the reasonable costs of establishing and maintaining the website required in section 207 of this act; and

(b) Provide the following information:

(i) The name of the data broker and its primary physical, email, and internet website addresses; and

(ii) Any information on how consumers can exercise the rights specified in section 204 of this act; and

(iii) Any additional information or explanation the data broker chooses to provide concerning its data collection and processing practices.

(3) A data broker that fails to register as required in this section is liable for: (a) A civil penalty of $50 for each day, not

to exceed a total of $10,000 for each year, it fails to register pursuant to this section; (b) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and (c) other penalties imposed by law.

NEW SECTION. **Sec. 203.** (1) A data broker may not process a consumer's sensitive data unless the consumer provides consent for the processing to the data broker.

(2) A data broker may not process a consumer's personal data in furtherance of profiling unless the consumer provides consent for the processing to the data broker.

(3) A data broker may not process a consumer's personal data in furtherance of the sale of personal data unless the consumer provides consent for the processing to the data broker.

NEW SECTION. **Sec. 204.** (1) A consumer has the right to confirm whether or not personal data concerning the consumer is being processed by or on behalf of a data broker and to access such personal data.

(2) A consumer has the right to correct inaccurate personal data concerning the consumer that is being processed by or on behalf of a data broker.

(3) A consumer has the right to delete personal data concerning the consumer that is being processed by or on behalf of a data broker.

NEW SECTION. **Sec. 205.** (1) A person may not acquire brokered personal data through fraudulent means.

(2) A person may not acquire or use brokered personal data in furtherance of: (a) Stalking or harassing another person; (b) committing a fraud, including identity theft, financial fraud, or email fraud; or (c) engaging in unlawful discrimination, including employment discrimination and housing discrimination.

NEW SECTION. **Sec. 206.** A data broker shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information. The data security practices must be appropriate to the volume and nature of the personal information at issue.

NEW SECTION. **Sec. 207.** The secretary of state shall create a web page on its internet website where the information provided by data brokers under this chapter is accessible to the public.

NEW SECTION. **Sec. 208.** The secretary of state may adopt rules as deemed necessary for the implementation and enforcement of this chapter.

NEW SECTION. **Sec. 209.** A court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this chapter if: (1) A series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this chapter, including the disclosure of information by a business to a third party in order to avoid the definition of "sell," "profiling," or "brokered personal data;" or (2) steps or transactions were taken to purposely avoid the definition of "sell" by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use.

NEW SECTION. **Sec. 210.** (1) Except as provided in subsection (2) of this section, nothing in this chapter creates an independent cause of action, except for the actions brought by the attorney general to enforce this chapter. Except as provided in subsection (2) of this section, no person, except for the attorney general, may enforce the rights and protections created by this chapter in any action. However, nothing in this chapter limits any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than this chapter, the person continues to have those rights and protections notwithstanding the existence of this chapter.

(2) A consumer alleging a violation of section 204 of this act may bring a civil action in any court of competent jurisdiction. Remedies are limited to appropriate injunctive relief necessary and proportionate to remedy the violation against the aggrieved consumer. The court shall also award reasonable attorneys' fees and costs

directly incurred in pursuit of claims under this act to any prevailing plaintiff.

NEW SECTION. **Sec. 211.** (1) Except as provided in section 209 of this act, this chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

(2) 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.

(3) The legislative declarations in this section do not apply to any claim or action by any party other than the attorney general alleging that conduct regulated by this chapter violates chapter 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

(4) In the event of a business's or service provider's violation under this chapter, prior to filing a complaint, the attorney general must provide the business or service provider 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 business or service provider has failed to cure any alleged violation, the attorney general may bring an action against the controller or processor as provided under this chapter.

(5) In determining a civil penalty under this chapter, the court must consider, as mitigating factors, a business's or service provider'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.

(6) All receipts from the imposition of civil penalties under this chapter must be deposited into the data broker registration account created in section 212 of this act.

NEW SECTION. **Sec. 212.** The data broker registration account is created in the custody of the state treasurer. All receipts collected under this chapter must be deposited into the account. Moneys in the account may be spent only after appropriation. Moneys in the account

may be used only for the implementation and enforcement of this chapter by the secretary of state and for the purposes of recovery of costs and attorneys' fees accrued by the attorney general in enforcing this chapter. Only the secretary of state, or the designee of the secretary of state, may authorize expenditures from this account. Moneys may not be used to supplant general fund appropriations to either agency.

PART 3
DO NOT TRACK MECHANISM

NEW SECTION. **Sec. 301.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Authenticate" means to use reasonable means to determine that a request to exercise the right in section 303(1) of this act is being made by the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(2) "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.

(3) "Consumer" means a natural person who is a Washington resident acting only in an individual or household context.

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

(5) "Do not track mechanism" means a technical mechanism, such as a control built into a web browser, an operating system, or a device, that permits a consumer to clearly communicate to websites, online applications, or other online services the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data that meets the technical specifications required pursuant to section 304 of this act.

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

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

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

(9)(a) "Personal data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

(b) "Personal data" includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

(ii) Characteristics of protected classifications under Washington state or federal law, as they may be construed or amended from time to time;

(iii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(iv) Biometric data;

(v) Internet or other electronic network activity information including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;

(vi) Sensitive data; and

(vii) Inferences drawn from any of the information identified in this subsection to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(c) "Personal data" does not include deidentified data.

(10) "Process" or "processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use,

storage, disclosure, sharing, analysis, deletion, or modification of personal data.

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

(12)(a) "Profiling" means any form of automated processing of personal information to evaluate, analyze, or predict personal aspects concerning a consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(b) "Profiling" does not include evaluation, analysis, or prediction based solely upon a consumer's current activity, including a consumer's current search query or current visit to a website or online application, if no personal data is retained after the completion of the activity for the purposes identified in (a) of this subsection.

(13)(a) "Publicly available information" means information that: (i) Is lawfully made available from federal, state, or local government records; (ii) a business has a reasonable basis to believe is lawfully made available to the general public from widely distributed media; or (iii) is directly and voluntarily disclosed to the general public by the individual to whom the information relates.

(b) "Publicly available information" does not mean: (i) Information derived from publicly available information; (ii) biometric data; or (iii) nonpublicly available information that has been combined with publicly available information.

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

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

transaction in which the third party assumes control of all or part of the controller's assets.

(15) "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 minor child; or (d) specific geolocation data. "Sensitive data" is a form of personal data.

(16) "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.

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

(18) "Targeted advertising" means advertising based upon profiling.

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

NEW SECTION. **Sec. 302.** (1) This chapter applies to legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) During a calendar year, controls or processes personal data of 100,000 consumers or more; or

(b) Derives over 25 percent of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.

(2) This chapter does not apply to:

(a) State agencies, legislative agencies, the judicial branch, local governments, or tribes; or

(b) Municipal corporations.

NEW SECTION. **Sec. 303.** (1) Beginning July 1, 2024, a consumer has the right to opt out of the processing of personal data

concerning such a consumer for the purposes of: (a) Targeted advertising; or (b) the sale of personal data.

(2) Beginning July 1, 2024, a controller that processes personal data for purposes of targeted advertising or the sale of personal data shall allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data pursuant to subsection (1) of this section through a user-selected do not track mechanism that meets the technical specifications established by the office of the attorney general pursuant to section 304 of this act.

(3)(a) Notwithstanding a consumer's decision to exercise the right to opt out of the processing of personal data through a do not track mechanism pursuant to subsection (2) of this section, a controller may enable the consumer to consent, through a web page, application, or a similar method, to the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data. This consent takes precedence over any choice reflected through a do not track mechanism.

(b) Before obtaining a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data pursuant to this subsection, a controller shall provide the consumer with a clear and conspicuous notice: (i) Informing the consumer about the choices available under this section; (ii) describing the categories of personal data to be processed and the purposes for which they will be processed; and (iii) explaining how and where the consumer may withdraw consent.

(c) The web page, application, or other means by which a controller obtains a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data must also allow the consumer to revoke the consent as easily as it is affirmatively provided.

NEW SECTION. **Sec. 304.** (1) By July 1, 2024, the office of the attorney general, in consultation with the office of privacy and data protection, must adopt rules, pursuant to chapter 34.05 RCW, establishing technical specifications for one or more do not track mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 303 of this act. These rules may be

revised as needed to reflect the means by which consumers interact with controllers.

(2) By July 1, 2023, to inform rule making, the office of the attorney general, in consultation with the office of privacy and data protection, must conduct an analysis of any do not track mechanism or any similar mechanism technical specifications required by law or regulation in the United States, including specifications for informing consumers about available opt-out choices and authenticating consumer requests, or requests made by a third party designated by a consumer, to opt out of processing for the purpose of targeted advertising or the sale of personal data pursuant to section 303 of this act. Additional stakeholders with relevant expertise may be consulted when conducting the analysis.

(3) In the rules adopted under this section, the office of the attorney general, in consultation with the office of privacy and data protection, must:

(a) Utilize the analysis conducted pursuant to subsection (2) of this section in order to develop technical specifications that are as consistent as reasonably possible with any other similar mechanism required by law or regulation in the United States;

(b) Provide technical specifications in plain, straightforward language; and

(c) Require mechanisms to clearly represent a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data pursuant to section 303 of this act.

(4) The rules adopted under this section must not: (a) Permit the manufacturer of a platform, browser, device, or any other product offering a do not track mechanism to unfairly disadvantage another controller; or (b) authorize a do not track mechanism that is a default setting.

NEW SECTION. **Sec. 305.** (1) Except as provided in subsection (2) of this section, nothing in this chapter creates an independent cause of action, except for the actions brought by the attorney general to enforce this chapter. Except as provided in subsection (2) of this section, no person, except for the attorney general, may enforce the rights and protections created by this chapter in any action. However, nothing in this chapter limits any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action.

The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than this chapter, the person continues to have those rights and protections notwithstanding the existence of this chapter.

(2) A consumer alleging a violation of section 303 of this act may bring a civil action in any court of competent jurisdiction. Remedies are limited to appropriate injunctive relief necessary and proportionate to remedy the violation against the aggrieved consumer. The court shall also award reasonable attorneys' fees and costs directly incurred in pursuit of claims under this act to any prevailing plaintiff.

NEW SECTION. **Sec. 306.** (1) Except as provided in section 110 of this act, this chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

(2) 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.

(3) The legislative declarations in this section do not apply to any claim or action by any party other than the attorney general alleging that conduct regulated by this chapter violates chapter 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

(4) In the event of a business's or service provider's violation under this chapter, prior to filing a complaint, the attorney general must provide the business or service provider 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 business or service provider has failed to cure any alleged violation, the attorney general may bring an action against the controller or processor as provided under this chapter.

(5) In determining a civil penalty under this chapter, the court must consider, as mitigating factors, a business's or service provider'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.

(6) All receipts from the imposition of civil penalties under this chapter must be deposited into the consumer privacy account created in section 112 of this act.

PART 4
MISCELLANEOUS

NEW SECTION. **Sec. 401.** (1) Sections 101 through 112 of this act constitute a new chapter in Title 19 RCW.

(2) Sections 201 through 212 of this act constitute a new chapter in Title 19 RCW.

(3) Sections 301 through 306 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 402.** Sections 101 through 113 and 201 through 211 of this act take effect July 1, 2023.

NEW SECTION. **Sec. 403.** 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.

--- END ---