

---

**SENATE BILL 5813**

---

**State of Washington**

**67th Legislature**

**2022 Regular Session**

**By** Senators Carlyle, Nguyen, Liias, Lovick, and Pedersen

Read first time 01/11/22. Referred to Committee on Environment,  
Energy & Technology.

1 AN ACT Relating to establishing data privacy protections to  
2 strengthen a consumer's ability to access, manage, and protect their  
3 personal data; adding a new section to chapter 42.56 RCW; adding new  
4 chapters to Title 19 RCW; creating a new section; prescribing  
5 penalties; and providing an effective date.

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

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

14 (2) Washington is a technology leader on a national and global  
15 level and recognizes its distinctive position in promoting the  
16 efficient balance of consumer privacy and economic benefits. Ongoing  
17 advances in technology have produced an exponential growth in the  
18 volume and variety of personal data being generated, collected,  
19 stored, and analyzed, which presents both promise and potential  
20 peril. The ability to harness and use data in positive ways is  
21 driving innovation and brings beneficial technologies to society.

1 However, it has also created risks to privacy and freedom. The  
2 unregulated and unauthorized use and disclosure of personal  
3 information and loss of privacy can have devastating impacts, ranging  
4 from financial fraud, identity theft, and unnecessary costs, to  
5 personal time and finances, to destruction of property, harassment,  
6 reputational damage, emotional distress, and physical harm.

7 (3) From a very young age, today's youth spend an extensive  
8 amount of their time engaged in online activities and services for  
9 various purposes including education, socializing, shopping, gaming,  
10 and entertainment. Children and adolescents navigate various websites  
11 and online applications without fully understanding what personal  
12 data is being collected about them, how this data can impact them in  
13 the future, or how to ensure the privacy and security of their  
14 personal data. The personal data of this vulnerable population  
15 requires and deserves additional protections, which includes parental  
16 or guardian oversight, adolescent control of data, and the ability  
17 for adults to delete their personal data from when they were a child  
18 or adolescent.

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

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

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

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

15 **PART 1**

16 **DATA RELATED TO CHILDREN AND ADOLESCENTS**

17  
18 NEW SECTION. **Sec. 101.** The definitions in this section apply  
19 throughout this chapter unless the context clearly requires  
20 otherwise.

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

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

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

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

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

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

11 (6) "Consent" means any freely given, specific, informed, and  
12 unambiguous indication of wishes of an adolescent or a parent or  
13 legal guardian of a child by which the adolescent or the parent or  
14 legal guardian of a child signifies agreement to the processing of  
15 personal data relating to the child or the adolescent for a narrowly  
16 defined particular purpose. Acceptance of a general or broad terms of  
17 use or similar document that contains descriptions of personal data  
18 processing along with other, unrelated information, does not  
19 constitute consent. Hovering over, muting, pausing, or closing a  
20 given piece of content does not constitute consent. Likewise,  
21 agreement obtained through dark patterns does not constitute consent.

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

25 (8) "Deidentified data" means data that cannot reasonably be used  
26 to infer information about, associate with, or otherwise link to a  
27 natural person, household, or a device linked to such a person or  
28 household, provided that the business that possesses the data: (a)  
29 Takes reasonable measures to ensure that the data cannot be used to  
30 infer information about, associate with, or otherwise link to, a  
31 natural person, household, or a device linked to such a person or  
32 household; (b) publicly commits to maintain and use the data only in  
33 a deidentified fashion and not attempt to reidentify the data; and  
34 (c) contractually obligates any recipients of the data to comply with  
35 all provisions of this subsection.

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

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

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

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

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

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

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

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

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

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

36 (iv) Biometric data;

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

1 (vi) Specific geolocation data;

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

4 (viii) Education information, defined as information that is not  
5 publicly available personally identifiable information as defined in  
6 the family educational rights and privacy act (20 U.S.C. Sec. 1232g,  
7 34 C.F.R. Part 99);

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

13 (x) Sensitive data.

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

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

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

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

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

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

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

7 (b) For the purposes of this chapter, a business does not sell  
8 personal data when: (i) An adolescent or a parent or legal guardian  
9 of a child provides consent to the business directing the business  
10 to: (A) Intentionally disclose personal data; or (B) intentionally  
11 interact with one or more third parties; (ii) the business discloses  
12 personal data to a service provider who processes the data on behalf  
13 of the business; or (iii) the business transfers to a third party the  
14 personal data of a child or an adolescent as an asset that is part of  
15 a merger, acquisition, bankruptcy, or other transaction in which the  
16 third party assumes control of all or part of the business, provided  
17 that personal data is used or shared consistently with this chapter.  
18 If a third party materially alters how it uses or shares the personal  
19 data of a child or an adolescent in a manner that is materially  
20 inconsistent with the promises made at the time of collection, it  
21 shall provide prior notice of the new or changed practice to the  
22 individual. The notice must be sufficiently prominent and robust to  
23 ensure that existing individuals can easily exercise their choices  
24 consistently with this chapter. This subsection does not authorize a  
25 business to make material, retroactive privacy policy changes or make  
26 other changes in their privacy policy in a manner that would violate  
27 the Washington consumer protection act, chapter 19.86 RCW.

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

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

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

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

18 (20) "Specific geolocation data" means data derived from  
19 technology including, but not limited to, global positioning system  
20 level latitude and longitude coordinates or other mechanisms that  
21 directly identifies the past or present physical location of a child  
22 or an adolescent or a device within a geographic area that is equal  
23 to or less than the area of a circle with a radius of 1,850 feet.  
24 Specific geolocation information excludes the content of  
25 communications.

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

30 (5) Except as provided in this chapter, a business may not  
31 process the personal data of a child or an adolescent for purposes  
32 that are not reasonably necessary to, or compatible with, the  
33 specified purposes for which the personal data is processed unless  
34 the business obtains the necessary consents as described in section  
35 102 of this act.

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

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

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

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

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

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

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

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

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

27 (3) The attorney general may request, in writing, that a business  
28 disclose any data protection assessment that is relevant to an  
29 investigation conducted by the attorney general. The business must  
30 make a data protection assessment available to the attorney general  
31 upon such a request. The attorney general may evaluate the data  
32 protection assessments for compliance with the responsibilities  
33 contained in this chapter and, if it serves a civil investigative  
34 demand, with RCW 19.86.110. Data protection assessments are  
35 confidential and exempt from public inspection and copying under  
36 chapter 42.56 RCW. The disclosure of a data protection assessment  
37 pursuant to a request from the attorney general under this subsection  
38 does not constitute a waiver of the attorney-client privilege or work  
39 product protection with respect to the assessment and any information

1 contained in the assessment unless otherwise subject to case law  
2 regarding the applicability of attorney-client privilege or work  
3 product protections.

4 (4) A data protection assessment conducted by a business for the  
5 purpose of compliance with other laws or regulations may qualify  
6 under this section if it has a similar scope and effect.

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

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

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

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

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

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

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

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

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

35 (3) The obligation to delete personal data pursuant to sections  
36 103(3), 104(3) or 105 of this act does not apply to publicly  
37 available information.

38 (4) Obligations imposed on a business under this chapter may not  
39 adversely affect the rights or freedoms of any persons, such as

1 exercising the right of free speech pursuant to the First Amendment  
2 to the United States Constitution.

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

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

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

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

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

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

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

8 (2) In actions brought by the attorney general, the legislature  
9 finds: (a) The practices covered by this chapter are matters vitally  
10 affecting the public interest for the purpose of applying the  
11 consumer protection act, chapter 19.86 RCW; and (b) a violation of  
12 this chapter is not reasonable in relation to the development and  
13 preservation of business, is an unfair or deceptive act in trade or  
14 commerce, and an unfair method of competition for the purpose of  
15 applying the consumer protection act, chapter 19.86 RCW.

16 (3) The legislative declarations in this section do not apply to  
17 any claim or action by any party other than the attorney general  
18 alleging that conduct regulated by this chapter violates chapter  
19 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

20 (4) In the event of a business's or service provider's violation  
21 under this chapter, prior to filing a complaint, the attorney general  
22 must provide the business or service provider with a warning letter  
23 identifying the specific provisions of this chapter the attorney  
24 general alleges have been or are being violated. If, after 30 days of  
25 issuance of the warning letter, the attorney general believes the  
26 business or service provider has failed to cure any alleged  
27 violation, the attorney general may bring an action against the  
28 controller or processor as provided under this chapter.

29 (5) In determining a civil penalty under this chapter, the court  
30 must consider, as mitigating factors, a business's or service  
31 provider's good faith efforts to comply with the requirements of this  
32 chapter and any actions to cure or remedy the violations before an  
33 action is filed.

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

37 NEW SECTION. **Sec. 112.** The consumer privacy account is created  
38 in the state treasury. All receipts from the imposition of civil



1 penalties under this chapter must be deposited into the account.  
2 Moneys in the account may be spent only after appropriation. Moneys  
3 in the account may only be used for the purposes of recovery of costs  
4 and attorneys' fees accrued by the attorney general in enforcing this  
5 chapter and for the office of privacy and data protection as created  
6 in RCW 43.105.369. Moneys may not be used to supplant general fund  
7 appropriations to either agency.

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

10 A data protection assessment submitted by a business to the  
11 attorney general in accordance with the requirements under section  
12 108 of this act is exempt from disclosure under this chapter.

13 **PART 2**  
14 **DATA BROKERS**

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

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

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

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

- 33 (i) Name;  
34 (ii) Address;  
35 (iii) Date of birth;  
36 (iv) Place of birth;  
37 (v) Mother's maiden name;

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

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

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

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

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

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

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

28 (5) "Consent" means any freely given, specific, informed, and  
29 unambiguous indication of the consumer's wishes by which the consumer  
30 signifies agreement to the processing of personal data relating to  
31 the consumer for a narrowly defined particular purpose. Acceptance of  
32 a general or broad terms of use or similar document that contains  
33 descriptions of personal data processing along with other, unrelated  
34 information, does not constitute consent. Hovering over, muting,  
35 pausing, or closing a given piece of content does not constitute  
36 consent. Likewise, agreement obtained through dark patterns does not  
37 constitute consent.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

39 (iv) Biometric data;

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

5 (vi) Specific geolocation data;

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

8 (viii) Education information, defined as information that is not  
9 publicly available personally identifiable information as defined in  
10 the family educational rights and privacy act (20 U.S.C. Sec. 1232g,  
11 34 C.F.R. Part 99);

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

17 (x) Sensitive data.

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

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

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

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

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

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

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

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

13 (b) For purposes of this chapter, a business does not sell  
14 personal data when: (i) A consumer provides consent to the business  
15 directing the business to: (A) Intentionally disclose personal data;  
16 or (B) intentionally interact with one or more third parties; (ii) it  
17 discloses personal data to a processor who processes the data on  
18 behalf of the business; or (iii) the business transfers to a third  
19 party the personal data of a consumer as an asset that is part of a  
20 merger, acquisition, bankruptcy, or other transaction in which the  
21 third party assumes control of all or part of the business, provided  
22 that data is used or shared consistently with this chapter. If a  
23 third party materially alters how it uses or shares the personal data  
24 of a consumer in a manner that is materially inconsistent with the  
25 promises made at the time of collection, it shall provide prior  
26 notice of the new or changed practice to the consumer. The notice  
27 must be sufficiently prominent and robust to ensure that existing  
28 consumers can easily exercise their choices consistently with this  
29 chapter. This subsection does not authorize a business to make  
30 material, retroactive privacy policy changes or make other changes in  
31 their privacy policy in a manner that would violate the Washington  
32 consumer protection act, chapter 19.86 RCW.

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

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

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

10 (19) "Specific geolocation data" means data derived from  
11 technology including, but not limited to, global positioning system  
12 level latitude and longitude coordinates or other mechanisms that  
13 directly identifies the past or present physical location of a  
14 natural person or a device within a geographic area that is equal to  
15 or less than the area of a circle with a radius of 1,850 feet.  
16 Specific geolocation data excludes the content of communications.

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

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

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

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

30 (b) Provide the following information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

6 (2) In actions brought by the attorney general, the legislature  
7 finds: (a) The practices covered by this chapter are matters vitally  
8 affecting the public interest for the purpose of applying the  
9 consumer protection act, chapter 19.86 RCW; and (b) a violation of  
10 this chapter is not reasonable in relation to the development and  
11 preservation of business, is an unfair or deceptive act in trade or  
12 commerce, and an unfair method of competition for the purpose of  
13 applying the consumer protection act, chapter 19.86 RCW.

14 (3) The legislative declarations in this section do not apply to  
15 any claim or action by any party other than the attorney general  
16 alleging that conduct regulated by this chapter violates chapter  
17 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

18 (4) In the event of a business's or service provider's violation  
19 under this chapter, prior to filing a complaint, the attorney general  
20 must provide the business or service provider with a warning letter  
21 identifying the specific provisions of this chapter the attorney  
22 general alleges have been or are being violated. If, after 30 days of  
23 issuance of the warning letter, the attorney general believes the  
24 business or service provider has failed to cure any alleged  
25 violation, the attorney general may bring an action against the  
26 controller or processor as provided under this chapter.

27 (5) In determining a civil penalty under this chapter, the court  
28 must consider, as mitigating factors, a business's or service  
29 provider's good faith efforts to comply with the requirements of this  
30 chapter and any actions to cure or remedy the violations before an  
31 action is filed.

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

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

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

8 **PART 3**

9 **DO NOT TRACK MECHANISM**

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

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

17 (2) "Consent" means any freely given, specific, informed, and  
18 unambiguous indication of the consumer's wishes by which the consumer  
19 signifies agreement to the processing of personal data relating to  
20 the consumer for a narrowly defined particular purpose. Acceptance of  
21 a general or broad terms of use or similar document that contains  
22 descriptions of personal data processing along with other, unrelated  
23 information, does not constitute consent. Hovering over, muting,  
24 pausing, or closing a given piece of content does not constitute  
25 consent.

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

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

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

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

3 (7) "Legislative agencies" has the same meaning as defined in RCW  
4 44.80.020.

5 (8) "Local government" has the same meaning as defined in RCW  
6 39.46.020.

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

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

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

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

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

26 (iv) Biometric data;

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

31 (vi) Sensitive data; and

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

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

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

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

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

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

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

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

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

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

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

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

3 (15) "Sensitive data" means: (a) Personal data revealing racial  
4 or ethnic origin, religious beliefs, mental or physical health  
5 condition or diagnosis, sexual orientation, or citizenship or  
6 immigration status; (b) the processing of genetic or biometric data  
7 for the purpose of uniquely identifying a natural person; (c) the  
8 personal data from a known minor child; or (d) specific geolocation  
9 data. "Sensitive data" is a form of personal data.

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

17 (17) "State agency" has the same meaning as defined in RCW  
18 43.105.020.

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

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

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

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

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

33 (2) This chapter does not apply to:

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

36 (b) Municipal corporations.

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

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

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

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

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

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

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

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

3 (2) By July 1, 2023, to inform rule making, the office of the  
4 attorney general, in consultation with the office of privacy and data  
5 protection, must conduct an analysis of any do not track mechanism or  
6 any similar mechanism technical specifications required by law or  
7 regulation in the United States, including specifications for  
8 informing consumers about available opt-out choices and  
9 authenticating consumer requests, or requests made by a third party  
10 designated by a consumer, to opt out of processing for the purpose of  
11 targeted advertising or the sale of personal data pursuant to section  
12 303 of this act. Additional stakeholders with relevant expertise may  
13 be consulted when conducting the analysis.

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

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

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

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

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

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



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

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

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

16 (2) In actions brought by the attorney general, the legislature  
17 finds: (a) The practices covered by this chapter are matters vitally  
18 affecting the public interest for the purpose of applying the  
19 consumer protection act, chapter 19.86 RCW; and (b) a violation of  
20 this chapter is not reasonable in relation to the development and  
21 preservation of business, is an unfair or deceptive act in trade or  
22 commerce, and an unfair method of competition for the purpose of  
23 applying the consumer protection act, chapter 19.86 RCW.

24 (3) The legislative declarations in this section do not apply to  
25 any claim or action by any party other than the attorney general  
26 alleging that conduct regulated by this chapter violates chapter  
27 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

28 (4) In the event of a business's or service provider's violation  
29 under this chapter, prior to filing a complaint, the attorney general  
30 must provide the business or service provider with a warning letter  
31 identifying the specific provisions of this chapter the attorney  
32 general alleges have been or are being violated. If, after 30 days of  
33 issuance of the warning letter, the attorney general believes the  
34 business or service provider has failed to cure any alleged  
35 violation, the attorney general may bring an action against the  
36 controller or processor as provided under this chapter.

37 (5) In determining a civil penalty under this chapter, the court  
38 must consider, as mitigating factors, a business's or service  
39 provider's good faith efforts to comply with the requirements of this

1 chapter and any actions to cure or remedy the violations before an  
2 action is filed.

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

6 **PART 4**  
7 **MISCELLANEOUS**

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

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

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

14 NEW SECTION. **Sec. 402.** Sections 101 through 113 and 201 through  
15 211 of this act take effect July 1, 2023.

16 NEW SECTION. **Sec. 403.** If any provision of this act or its  
17 application to any person or circumstance is held invalid, the  
18 remainder of the act or the application of the provision to other  
19 persons or circumstances is not affected.

--- END ---