

---

**HOUSE BILL 1433**

---

**State of Washington**

**67th Legislature**

**2021 Regular Session**

**By** Representatives Kloba, Sutherland, Ryu, J. Johnson, Valdez, Dolan, Young, Ramel, Bergquist, Eslick, Jacobsen, and Harris-Talley

Read first time 02/01/21. Referred to Committee on Civil Rights & Judiciary.

1 AN ACT Relating to creating a charter of people's personal data  
2 rights; adding a new chapter to Title 19 RCW; and prescribing  
3 penalties.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

29        (2) "Captured personal information" means personal information  
30 about a Washington resident that is captured in an interaction in  
31 which a covered entity directly or indirectly makes available  
32 information, products, or services to an individual or household.  
33 Covered interactions include but are not limited to posting of  
34 information, offering of a product or service, the placement of  
35 targeted advertisements, or offering a membership or other ongoing  
36 relationship with an entity. For the purposes of this chapter,  
37 "captured personal information" includes biometric information,  
38 regardless of how captured.

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

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

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

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

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

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

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

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

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

31 (d) Not attempt to reidentify the information; and

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

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

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

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

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

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

13 (a) Direct or indirect financial harm;

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

17 (c) Discrimination in products, services, or economic  
18 opportunity, such as housing, employment, credit, insurance,  
19 education, or health care, on the basis of an individual or class of  
20 individuals' actual or perceived age, race, national origin, sex,  
21 sexual orientation, gender identity, disability, and/or membership in  
22 another protected class, except as specifically authorized by law;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 (20) "Washington governmental entity" shall mean a department or  
18 agency of Washington state or a political subdivision thereof,  
19 including but not limited to public authorities and special use  
20 districts, or an individual acting for or on behalf of the state or a  
21 political subdivision thereof.

22 NEW SECTION. **Sec. 4.** An individual residing in Washington state  
23 has the following rights with regard to the individual's personal  
24 information:

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

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

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

35 (4) The right to correct inaccurate personal information;

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

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

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

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

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

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

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

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

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

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

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

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

33 (ii) Be clear and prominent in appearance;

34 (iii) Use clear and plain language;

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

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



1 (vi) Be understandable by the least sophisticated consumer;  
2 (vii) Be clearly distinguishable from other matters;  
3 (viii) Not contain any unrelated, confusing, or contradictory  
4 information;  
5 (ix) Be no more than 500 words, excluding the list of third  
6 parties with which the covered entity discloses captured personal  
7 information, as required under (c)(vi) of this subsection; and  
8 (x) Be provided free of charge.

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

11 (i) What captured personal information is being processed;  
12 (ii) The manner in which the captured personal information is  
13 processed;  
14 (iii) How and for what purpose the covered entity processes the  
15 captured personal information;  
16 (iv) How long the captured personal information will be retained;  
17 (v) Whether and how the covered entity monetizes captured  
18 personal information;  
19 (vi) To what types of third parties the covered entity discloses  
20 captured personal information and for what purposes; and  
21 (vii) How the covered entity collects captured personal  
22 information, including offline practices, including but not limited  
23 to when the individual is not interacting directly with the covered  
24 entity.

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

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

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

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

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

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

11 (2) Opt-in consent.

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

- 14 (i) Process the individual's captured personal information; or
- 15 (ii) Make any changes in the processing of the individual's  
16 captured personal information that would necessitate a change to the  
17 information required to be provided under subsection (1)(c) of this  
18 section.

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

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

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

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

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

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

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

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

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

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

15 (h) A covered entity shall not discriminate against individuals  
16 by reason of their not granting opt-in consent to the processing of  
17 their personal information under this chapter or otherwise exercising  
18 their rights under this chapter, including but not limited to, by:  
19 Denying goods or services to the individual; charging different  
20 prices or rates for goods or services, including through the use of  
21 discounts or other benefits or imposing penalties; providing a  
22 different level or quality of goods or services to the individual;  
23 and suggesting that the individual will receive a different price or  
24 rate for goods or services or a different level or quality of goods  
25 or services. Notwithstanding the above, a covered entity may, with  
26 the individual's opt-in consent given in compliance with this  
27 subsection (2), operate a program in which information, products or  
28 services sold to the individual are discounted based on that  
29 individual's prior purchases from the covered entity, provided that  
30 the captured personal information shall be processed solely for the  
31 purpose of operating such program.

32 (i) A covered entity shall not state or imply that the quality of  
33 a product or service will be diminished and shall not actually  
34 diminish the quality of a product or service if the individual  
35 declines to give opt-in consent to captured personal information  
36 processing.

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

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

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

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

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

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

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

26 (3) Obligation of care.

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

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

38 (4) Access to personal information.

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

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

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

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

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

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

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

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

27 (i) Clear and conspicuous;

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

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

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

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

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

5 (5) Correction and deletion of personal information.

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

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

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

22 (i) Clear and conspicuous;

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

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

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

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

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

40 (6) Confidentiality and protection of data.

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

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

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

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

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

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

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

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

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

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

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

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

9 (7) Surreptitious surveillance.

10 A covered entity shall not activate the microphone, camera, or  
11 any other sensor on a device in the lawful possession of an  
12 individual that is capable of collecting or transmitting personal  
13 information, without providing the privacy notices required in  
14 subsection (1) of this section and obtaining the individual's freely  
15 given, specific, informed, and unambiguous opt-in consent pursuant to  
16 subsection (2) of this section for the specific type of measurement  
17 to be activated; provided that such opt-in consent shall be effective  
18 for no more than 90 days after which it shall expire unless renewed  
19 by the individual's freely given, specific, informed, and unambiguous  
20 opt-in consent pursuant to subsection (2) of this section.

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

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

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

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

32 (1) **Retention; disclosure; destruction.** A covered entity or  
33 Washington governmental entity that processes biometric information  
34 must develop a written policy, made available to the public,  
35 establishing a retention schedule and guidelines for permanently  
36 destroying biometric information when the initial purpose for  
37 processing such information has been satisfied or within one year of  
38 the individual's last interaction with the covered entity or



1 Washington governmental entity, whichever occurs first. Consent under  
2 subsection (2) of this section shall be for a period specified in the  
3 written consent of not more than one year, and shall automatically  
4 expire at the end of such period unless renewed pursuant to  
5 subsection (2) of this section. Upon expiration of consent, any  
6 biometric information possessed by a covered entity or Washington  
7 governmental entity must be destroyed. Absent a valid warrant issued  
8 by a court of competent jurisdiction, a covered entity or Washington  
9 governmental entity in possession of biometric information must  
10 comply with its established retention schedule and destruction  
11 guidelines.

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

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

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

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

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

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

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

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

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

37 (d) The disclosure is required pursuant to a valid warrant or  
38 subpoena issued by a court of competent jurisdiction or a subpoena  
39 issued by a governmental entity or in a pending judicial case,  
40 provided that in the case of a subpoena the entity subject to the

1 subpoena shall postpone compliance therewith until it has given the  
2 subject of the subpoena notice of the facts set forth in section  
3 9(2)(b)(i) of this act has allowed at least 10 business days for the  
4 subject to seek review of or otherwise challenge the subpoena.

5 (4) **Monetizing.** No covered entity or Washington governmental  
6 entity in possession of biometric information may monetize, or  
7 otherwise profit from an individual's biometric information; provided  
8 only that a covered entity may process an individual's biometric  
9 information, with full disclosure and opt-in consent consistent with  
10 section 5(2) of this act, in a service in which the covered entity  
11 reports to the individual the biometric information processed and/or  
12 utilizes the biometric information to design or recommend actions or  
13 products that have been specifically requested by the individual with  
14 full disclosure that such recommendation is based on the biometric  
15 information processed, provided that the biometric information shall  
16 not be used for any other purpose.

17 (5) **Identification.** Notwithstanding any other provision of this  
18 chapter, a covered entity or governmental entity may list personal  
19 information such as name or birthdate and biometric information such  
20 as height, weight, or photograph on an issued license, membership or  
21 identification card for the sole purpose of allowing an employee or  
22 other representative of the covered entity to determine based solely  
23 on personal observation, and without the assistance of technologies  
24 such as facial recognition, whether the person physically holding  
25 such license or card is the person entitled to hold it, provided  
26 further that such intended use is disclosed to the individual prior  
27 to capturing the biometric information. Any other processing of such  
28 biometric information shall be subject to all the terms and  
29 conditions of this chapter. Any covered entity or governmental entity  
30 using personal information or biometric information under this  
31 subsection must ensure that it is not stored or processed in any  
32 manner that would allow a third party to process such information for  
33 any purpose.

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

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

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

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

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

29 (d) For a covered entity or Washington governmental entity to  
30 operate, install, or commission the operation or installation of  
31 equipment incorporating face recognition in any place of public  
32 resort, accommodation, assemblage, or amusement, as defined in RCW  
33 49.60.040. For the purpose of this subsection, "face recognition"  
34 means: (i) An automated or semiautomated process by which an  
35 individual is identified or attempted to be identified based on the  
36 characteristics of the individual's face; or (ii) an automated or  
37 semiautomated process by which the characteristics of an individual's  
38 face are analyzed to determine the individual's sentiment, state of  
39 mind, or other propensities including, but not limited to, the  
40 person's level of dangerousness;

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

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

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

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

1 a package. However, captured personal information shall not be  
2 processed for any other purpose beyond that clear primary purpose  
3 without the freely given, specific, informed, and unambiguous opt-in  
4 consent from the individual to whom the captured personal information  
5 pertains, except as required by law.

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

11 (a) It believes that an emergency involving immediate danger of  
12 death or serious physical injury to any individual requires obtaining  
13 without delay captured personal information related to the emergency  
14 and the request is narrowly tailored to address the emergency,  
15 subject to the following limitations:

16 (i) The request shall document the factual basis for believing  
17 that an emergency involving immediate danger of death or serious  
18 physical injury to an individual requires obtaining without delay  
19 captured personal information relating to the emergency; and

20 (ii) Simultaneous with the covered entity or Washington  
21 governmental entity obtaining captured personal information under  
22 this subsection (a), the covered entity or Washington governmental  
23 entity shall use reasonable efforts to inform the individual of the  
24 captured personal information obtained; the details of the emergency;  
25 and the reasons why the covered entity or Washington governmental  
26 entity needed to use, access, or disclose the biometric information  
27 and shall continue such efforts to inform until receipt of  
28 information is confirmed; and

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

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

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

3 (B) That captured personal information maintained for the  
4 individual was supplied to or requested by the requesting entity and  
5 the date on which the supplying or request took place;

6 (C) An inventory of the captured personal information requested  
7 or supplied; and

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

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

19 (iii) In the case of a subpoena, a covered entity subject to a  
20 subpoena shall postpone compliance therewith until it has given the  
21 subject of the subpoena notice of the information required under this  
22 subsection (2)(b)(i) and has allowed at least 10 business days for  
23 the subject to seek review of or otherwise challenge the subpoena;

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

25 (d) Processing involves only deidentified information.

26 (3) This chapter shall not apply to captured personal information  
27 captured from a patient by a health care provider or health care  
28 facility as defined in RCW 48.41.030 or biometric information  
29 collected, used, or stored exclusively for medical education or  
30 research, public health or epidemiological purposes, health care  
31 treatment, insurance, payment, or operations under the federal health  
32 insurance portability and accountability act of 1996, or to X-ray,  
33 roentgen process, computed tomography, magnetic resonance imaging,  
34 positron emission tomography scan, mammography, or other image or  
35 film of the human anatomy used exclusively to diagnose, prognose, or  
36 treat an illness or other medical condition or to further validate  
37 scientific testing or screening.

38 (4) To the extent the transaction requested by an individual is a  
39 covered entity's placement of that individual's personal information  
40 in the public domain, such as recording of a real estate deed showing

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

3 (5) This chapter shall not apply to individuals sharing their  
4 personal contact information such as email addresses with other  
5 individuals in workplace, social, political or similar settings where  
6 the purpose of the information is to facilitate communication among  
7 such individuals, provided that any processing of such contact  
8 information beyond interpersonal communication shall be covered by  
9 this chapter. This chapter shall not apply to entities' publication  
10 of entity-based member or employee contact information where such  
11 publication is intended to allow members of the public to contact  
12 such member or employee in the ordinary course of the entity's  
13 operations.

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

16 NEW SECTION. **Sec. 10.** (1) Private right of action.

17 (a) Any individual alleging a violation of this chapter or a  
18 regulation adopted under this chapter may bring a civil action in any  
19 court of competent jurisdiction. An individual protected by this  
20 chapter may not be required, as a condition of service or otherwise,  
21 to accept mandatory arbitration of a claim under this chapter.

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

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

28 (i) Liquidated damages of \$10,000 per violation or actual  
29 damages, whichever is greater;

30 (ii) Punitive damages; and

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

33 (d) In addition to any relief awarded pursuant to (c) of this  
34 subsection, the court shall award reasonable attorneys' fees and  
35 costs to any prevailing plaintiff.

36 (2)(a) The attorney general may bring an action in the name of  
37 the state, or as parens patriae on behalf of persons residing in the  
38 state, to enforce this chapter. For actions brought by the attorney  
39 general to enforce this chapter, the legislature finds that the

1 practices covered by this chapter are matters vitally affecting the  
2 public interest for the purpose of applying the consumer protection  
3 act, chapter 19.86 RCW. For actions brought by the attorney general  
4 to enforce this section, a violation of this section is not  
5 reasonable in relation to the development and preservation of  
6 business and is an unfair or deceptive act in trade or commerce and  
7 an unfair method of competition for purposes of applying the consumer  
8 protection act, chapter 19.86 RCW. An action to enforce this section  
9 may not be brought under RCW 19.86.090.

10 (b) In an action brought by the attorney general, the court may  
11 award:

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

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

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

20 (iv) Any other relief the court determines appropriate.

21 (3)(a) A city attorney or county prosecutor in a city or county  
22 having a population in excess of 200,000, may bring an action to  
23 enforce this chapter on behalf of the residents of such city or  
24 county.

25 (b) In an action brought by a district attorney or a city  
26 attorney, the court may award:

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

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

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

35 (iv) Any other relief the court determines appropriate.

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

39 (5) Each individual whose captured personal information was  
40 unlawfully processed, each instance of processing counts as a



1 separate violation. Each provision of this chapter that was violated  
2 counts as a separate violation.

3 (6) It is a violation of this chapter for a covered entity,  
4 Washington governmental entity, or anyone else acting on behalf of a  
5 covered entity or Washington governmental entity to retaliate against  
6 an individual who makes a good-faith complaint that there has been a  
7 failure to comply with any part of this chapter. An individual who is  
8 injured by a violation of this subsection (6) may bring a civil  
9 action for monetary damages and injunctive relief in any court of  
10 competent jurisdiction.

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

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

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

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

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

37 NEW SECTION. **Sec. 11.** (1) This chapter shall not supersede  
38 local or state laws, regulations, or ordinances except to the extent  
39 that it provides stronger privacy protections for individuals.

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

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

10           NEW SECTION.   **Sec. 12.**   If any provision of this act or its  
11 application to any person or circumstance is held invalid, the  
12 remainder of the act or the application of the provision to other  
13 persons or circumstances is not affected.

14           NEW SECTION.   **Sec. 13.**   Sections 1 through 11 of this act  
15 constitute a new chapter in Title 19 RCW.

--- END ---