

**2SSB 6281** - H COMM AMD

By Committee on Innovation, Technology & Economic Development

1 Strike everything after the enacting clause and insert the  
2 following:

3 "NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and  
4 cited as the Washington privacy act.

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

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

23 (3) Given that technological innovation and new uses of data can  
24 help solve societal problems and improve quality of life, the  
25 legislature seeks to shape responsible public policies where  
26 innovation and protection of individual privacy coexist. The  
27 legislature notes that our federal authorities have not developed or  
28 adopted into law regulatory or legislative solutions that give  
29 consumers control over their privacy. In contrast, the European  
30 Union's general data protection regulation has continued to influence  
31 data privacy policies and practices of those businesses competing in

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

5 (4) With this act, Washington state will be among the first tier  
6 of states giving consumers the ability to protect their own rights to  
7 privacy and requiring companies to be responsible custodians of data  
8 as technological innovations emerge. This act does so by explicitly  
9 providing consumers the right to access, correction, and deletion of  
10 personal data, as well as the right to opt out of the collection and  
11 use of personal data for certain purposes. These rights will add to,  
12 and not subtract from, the consumer protection rights that consumers  
13 already have under Washington state law.

14 (5) Additionally, this act imposes affirmative obligations upon  
15 companies to safeguard personal data and provide clear,  
16 understandable, and transparent information to consumers about how  
17 their personal data are used. It strengthens compliance and  
18 accountability by requiring data protection assessments in the  
19 collection and use of personal data. Finally, it empowers the state  
20 attorney general to obtain and evaluate a company's data protection  
21 assessments, to impose penalties where violations occur, and to  
22 prevent against future violations.

23 (6) The legislature also encourages the state office of privacy  
24 and data protection to monitor the development of universal privacy  
25 controls that communicate a consumer's affirmative, freely given, and  
26 unambiguous choice to opt out of the processing of personal data  
27 concerning the consumer for the purposes of targeted advertising, the  
28 sale of personal data, or profiling in furtherance of decisions that  
29 produce legal effects concerning the consumer or similarly  
30 significant effects concerning consumers.

31 (7) The legislature recognizes the unique business needs of  
32 institutions of higher education and nonprofit corporations. However,  
33 these entities control and process an extraordinary amount of  
34 personal data and consumers should be afforded the rights provided by  
35 this act regarding personal data. Therefore, it is the intent of the  
36 legislature to delay the date of application for these entities by  
37 three years in order to provide sufficient time to develop a plan to  
38 comply with the provisions of this act.

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

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

12        (2) "Authenticate" means to use reasonable means to determine  
13 that a request to exercise any of the rights in section 6 (1) through  
14 (4) of this act is being made by the consumer who is entitled to  
15 exercise such rights with respect to the personal data at issue.

16        (3) "Business associate" has the same meaning as in Title 45  
17 C.F.R., established pursuant to the federal health insurance  
18 portability and accountability act of 1996.

19        (4) "Child" means any natural person under thirteen years of age.

20        (5) "Consent" means a clear affirmative act signifying a freely  
21 given, specific, informed, and unambiguous indication of a consumer's  
22 agreement to the processing of personal data relating to the  
23 consumer, such as by a written statement, including by electronic  
24 means, or other clear affirmative action.

25        (6) "Consumer" means a natural person who is a Washington  
26 resident acting only in an individual or household context, including  
27 buying and selling in an individual or household context. It does not  
28 include a natural person acting in a commercial or employment  
29 context.

30        (7) "Controller" means the natural or legal person which, alone  
31 or jointly with others, determines the purposes and means of the  
32 processing of personal data.

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

36        (9) "Decisions that produce legal effects concerning a consumer  
37 or similarly significant effects concerning a consumer" means  
38 decisions that result in the provision or denial of financial and  
39 lending services, housing, insurance, education enrollment, criminal

1 justice, employment opportunities, health care services, or access to  
2 basic necessities, such as food and water.

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

12 (11) "Enroll," "enrolled," or "enrolling" means the process by  
13 which a facial recognition service creates a facial template from one  
14 or more images of a consumer and adds the facial template to a  
15 gallery used by the facial recognition service for identification,  
16 verification, or persistent tracking of consumers. It also includes  
17 the act of adding an existing facial template directly into a gallery  
18 used by a facial recognition service.

19 (12) "Facial recognition service" means technology that analyzes  
20 facial features and is used for the identification, verification, or  
21 persistent tracking of consumers in still or video images.

22 (13) "Facial template" means the machine-interpretable pattern of  
23 facial features that is extracted from one or more images of a  
24 consumer by a facial recognition service.

25 (14) "Health care facility" has the same meaning as in RCW  
26 70.02.010.

27 (15) "Health care information" has the same meaning as in RCW  
28 70.02.010.

29 (16) "Health care provider" has the same meaning as in RCW  
30 70.02.010.

31 (17) "Identification" means the use of a facial recognition  
32 service by a controller to determine whether an unknown consumer  
33 matches any consumer whose identity is known to the controller and  
34 who has been enrolled by reference to that identity in a gallery used  
35 by the facial recognition service.

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

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

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

1 (21) "Meaningful human review" means review or oversight by one  
2 or more individuals who are trained in accordance with section 17(8)  
3 of this act and who have the authority to alter the decision under  
4 review.

5 (22) "Nonprofit corporation" has the same meaning as in RCW  
6 24.03.005.

7 (23) "Ongoing surveillance" means tracking the physical movements  
8 of a specified individual through one or more public places over  
9 time, whether in real time or through application of a facial  
10 recognition service to historical records. It does not include a  
11 single recognition or attempted recognition of an individual if no  
12 attempt is made to subsequently track that individual's movement over  
13 time after the individual has been recognized.

14 (24) "Persistent tracking" means the use of a facial recognition  
15 service to track the movements of a consumer on a persistent basis  
16 without identification or verification of that consumer. Such  
17 tracking becomes persistent as soon as:

18 (a) The facial template that permits the tracking uses a facial  
19 recognition service for more than forty-eight hours after the first  
20 enrolling of that template; or

21 (b) The data created by the facial recognition service in  
22 connection with the tracking of the movements of the consumer are  
23 linked to any other data such that the consumer who has been tracked  
24 is identified or identifiable.

25 (25)(a) "Personal data" means any information that is linked or  
26 reasonably linkable to an identified or identifiable natural person.  
27 "Personal data" does not include deidentified data or publicly  
28 available information.

29 (b) For purposes of this subsection, "publicly available  
30 information" means information that is lawfully made available from  
31 federal, state, or local government records.

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

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

39 (28) "Profiling" means any form of automated processing of  
40 personal data to evaluate, analyze, or predict personal aspects

1 concerning an identified or identifiable natural person's economic  
2 situation, health, personal preferences, interests, reliability,  
3 behavior, location, or movements.

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

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

13 (31) "Recognition" means the use of a facial recognition service  
14 to determine whether:

15 (a) An unknown consumer matches any consumer who has been  
16 enrolled in a gallery used by the facial recognition service; or

17 (b) An unknown consumer matches a specific consumer who has been  
18 enrolled in a gallery used by the facial recognition service.

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

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

35 (33) "Security or safety purpose" means physical security,  
36 protection of consumer data, safety, fraud prevention, or asset  
37 protection.

38 (34) "Sensitive data" means (a) personal data revealing racial or  
39 ethnic origin, religious beliefs, mental or physical health condition  
40 or diagnosis, sexual orientation, or citizenship or immigration

1 status; (b) the processing of genetic or biometric data for the  
2 purpose of uniquely identifying a natural person; (c) the personal  
3 data from a known child; or (d) specific geolocation data. "Sensitive  
4 data" is a form of personal data.

5 (35) "Serious criminal offense" means any felony under chapter  
6 9.94A RCW or an offense enumerated by Title 18 U.S.C. Sec. 2516.

7 (36) "Specific geolocation data" means information derived from  
8 technology, including, but not limited to, global positioning system  
9 level latitude and longitude coordinates or other mechanisms, that  
10 directly identifies the specific location of a natural person with  
11 the precision and accuracy below one thousand seven hundred fifty  
12 feet. Specific geolocation data excludes the content of  
13 communications.

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

15 (38) "Targeted advertising" means displaying advertisements to a  
16 consumer where the advertisement is selected based on personal data  
17 obtained from a consumer's activities over time and across  
18 nonaffiliated web sites or online applications to predict such  
19 consumer's preferences or interests. It does not include advertising:  
20 (a) Based on activities within a controller's own web sites or online  
21 applications; (b) based on the context of a consumer's current search  
22 query or visit to a web site or online application; or (c) to a  
23 consumer in response to the consumer's request for information or  
24 feedback.

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

28 (40) "Verification" means the use of a facial recognition service  
29 by a controller to determine whether a consumer is a specific  
30 consumer whose identity is known to the controller and who has been  
31 enrolled by reference to that identity in a gallery used by the  
32 facial recognition service.

33 NEW SECTION. **Sec. 4.** JURISDICTIONAL SCOPE. (1) This chapter  
34 applies to legal entities that conduct business in Washington or  
35 produce products or services that are targeted to residents of  
36 Washington, and that satisfy one or more of the following thresholds:

37 (a) During a calendar year, controls or processes personal data  
38 of one hundred thousand consumers or more; or

1 (b) Derives over twenty-five percent of gross revenue from the  
2 sale of personal data and processes or controls personal data of  
3 twenty-five thousand consumers or more.

4 (2) This chapter does not apply to:

5 (a) State agencies, local governments, or tribes;

6 (b) Municipal corporations;

7 (c) Information that meets the definition of:

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

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

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

14 (iv) Identifiable private information for purposes of the federal  
15 policy for the protection of human subjects, 45 C.F.R. Part 46;  
16 identifiable private information that is otherwise information  
17 collected as part of human subjects research pursuant to the good  
18 clinical practice guidelines issued by the international council for  
19 harmonisation; the protection of human subjects under 21 C.F.R. Parts  
20 50 and 56; or personal data used or shared in research conducted in  
21 accordance with one or more of the requirements set forth in this  
22 subsection;

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

25 (A) A quality improvement committee for purposes of RCW  
26 43.70.510, 70.230.080, or 70.41.200;

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

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

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

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

37 (vii) Patient safety work product for purposes of 42 C.F.R. Part  
38 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

39 (viii) Information that is (A) deidentified in accordance with  
40 the requirements for deidentification set forth in 45 C.F.R. Part



1 164, and (B) derived from any of the health care-related information  
2 listed in this subsection (2)(c);

3 (d) Information originating from, and intermingled to be  
4 indistinguishable with, information under (c) of this subsection that  
5 is maintained by:

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

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

11 (iii) A program or a qualified service organization as defined by  
12 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

15 (f)(i) An activity involving the collection, maintenance,  
16 disclosure, sale, communication, or use of any personal information  
17 bearing on a consumer's credit worthiness, credit standing, credit  
18 capacity, character, general reputation, personal characteristics, or  
19 mode of living by a consumer reporting agency, as defined in Title 15  
20 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in  
21 Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a  
22 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by  
23 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.  
24 1681b.

25 (ii) (f)(i) of this subsection shall apply only to the extent  
26 that such activity involving the collection, maintenance, disclosure,  
27 sale, communication, or use of such information by that agency,  
28 furnisher, or user is subject to regulation under the fair credit  
29 reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the information  
30 is not collected, maintained, used, communicated, disclosed, or sold  
31 except as authorized by the fair credit reporting act;

32 (g) Personal data collected and maintained for purposes of  
33 chapter 43.71 RCW;

34 (h) Personal data collected, processed, sold, or disclosed  
35 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and  
36 implementing regulations, if the collection, processing, sale, or  
37 disclosure is in compliance with that law;

38 (i) Personal data collected, processed, sold, or disclosed  
39 pursuant to the federal driver's privacy protection act of 1994 (18

1 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or  
2 disclosure is in compliance with that law;

3 (j) Personal data regulated by the federal family educations  
4 rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing  
5 regulations;

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

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

13 (m) Data maintained for employment records purposes.

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

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

22 NEW SECTION. **Sec. 5.** RESPONSIBILITY ACCORDING TO ROLE. (1)

23 Controllers and processors are responsible for meeting their  
24 respective obligations established under this chapter.

25 (2) Processors are responsible under this chapter for adhering to  
26 the instructions of the controller and assisting the controller to  
27 meet its obligations under this chapter. Such assistance shall  
28 include the following:

29 (a) Taking into account the nature of the processing, the  
30 processor shall assist the controller by appropriate technical and  
31 organizational measures, insofar as this is possible, for the  
32 fulfillment of the controller's obligation to respond to consumer  
33 requests to exercise their rights pursuant to section 6 of this act;  
34 and

35 (b) Taking into account the nature of processing and the  
36 information available to the processor, the processor shall assist  
37 the controller in meeting the controller's obligations in relation to  
38 the security of processing the personal data and in relation to the  
39 notification of a breach of the security of the system pursuant to

1 RCW 19.255.010; and shall provide information to the controller  
2 necessary to enable the controller to conduct and document any data  
3 protection assessments required by section 9 of this act.

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

6 (a) Implement and maintain reasonable security procedures and  
7 practices to protect personal data, taking into account the context  
8 in which the personal data are to be processed;

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

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

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

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

29 (b) (i) The processor shall make available to the controller all  
30 information necessary to demonstrate compliance with the obligations  
31 in this chapter; and (ii) the processor shall allow for, and  
32 contribute to, reasonable audits and inspections by the controller or  
33 the controller's designated auditor; alternatively, the processor  
34 may, with the controller's consent, arrange for a qualified and  
35 independent auditor to conduct, at least annually and at the  
36 processor's expense, an audit of the processor's policies and  
37 technical and organizational measures in support of the obligations  
38 under this chapter using an appropriate and accepted control standard  
39 or framework and audit procedure for such audits as applicable, and  
40 shall provide a report of such audit to the controller upon request.

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

4 (6) Determining whether a person is acting as a controller or  
5 processor with respect to a specific processing of data is a fact-  
6 based determination that depends upon the context in which personal  
7 data are to be processed. A person that is not limited in its  
8 processing of personal data pursuant to a controller's instructions,  
9 or that fails to adhere to such instructions, is a controller and not  
10 a processor with respect to a specific processing of data. A  
11 processor that continues to adhere to a controller's instructions  
12 with respect to a specific processing of personal data remains a  
13 processor. If a processor begins, alone or jointly with others,  
14 determining the purposes and means of the processing of personal  
15 data, it is a controller with respect to such processing.

16 NEW SECTION. **Sec. 6.** CONSUMER PERSONAL DATA RIGHTS. Consumers  
17 may exercise the rights set forth in this section by submitting a  
18 request, at any time, to a controller specifying which rights the  
19 consumer wishes to exercise. In the case of processing personal data  
20 concerning a known child, the parent or legal guardian of the known  
21 child shall exercise the rights of this chapter on the child's  
22 behalf. Where a controller processes personal data concerning a  
23 consumer subject to guardianship, conservatorship, or other  
24 protective arrangement under chapter 11.130 RCW, the controller must  
25 allow the guardian or the conservator to exercise the rights of this  
26 chapter on the consumer's behalf. Except as provided in this chapter,  
27 the controller must comply with a request to exercise the rights  
28 pursuant to subsections (1) through (5) of this section.

29 (1) *Right of access.* A consumer has the right to confirm whether  
30 or not a controller is processing personal data concerning the  
31 consumer and access such personal data.

32 (2) *Right to correction.* A consumer has the right to correct  
33 inaccurate personal data concerning the consumer, taking into account  
34 the nature of the personal data and the purposes of the processing of  
35 the personal data.

36 (3) *Right to deletion.* A consumer has the right to delete  
37 personal data concerning the consumer.

38 (4) *Right to data portability.* A consumer has the right to obtain  
39 personal data concerning the consumer, which the consumer previously

1 provided to the controller, in a portable and, to the extent  
2 technically feasible, readily usable format that allows the consumer  
3 to transmit the data to another controller without hindrance, where  
4 the processing is carried out by automated means.

5 (5) *Right to opt out.* A consumer has the right to opt out of the  
6 processing of personal data concerning such consumer for purposes of  
7 targeted advertising, the sale of personal data, or profiling in  
8 furtherance of decisions that produce legal effects concerning a  
9 consumer or similarly significant effects concerning a consumer.

10 (6) *Responding to consumer requests.* (a) A controller must inform  
11 a consumer of any action taken on a request under subsections (1)  
12 through (5) of this section without undue delay and in any event  
13 within forty-five days of receipt of the request. That period may be  
14 extended once by forty-five additional days where reasonably  
15 necessary, taking into account the complexity and number of the  
16 requests. The controller must inform the consumer of any such  
17 extension within forty-five days of receipt of the request, together  
18 with the reasons for the delay.

19 (b) If a controller does not take action on the request of a  
20 consumer, the controller must inform the consumer without undue delay  
21 and at the latest within forty-five days of receipt of the request of  
22 the reasons for not taking action and instructions for how to appeal  
23 the decision with the controller as described in subsection (7) of  
24 this section.

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

33 (d) A controller is not required to comply with a request to  
34 exercise any of the rights under subsections (1) through (4) of this  
35 section if the controller is unable to authenticate the request using  
36 commercially reasonable efforts. In such cases, the controller may  
37 request the provision of additional information reasonably necessary  
38 to authenticate the request.

39 (7) (a) Controllers must establish an internal process whereby  
40 consumers may appeal a refusal to take action on a request to

1 exercise any of the rights under subsections (1) through (5) of this  
2 section within a reasonable period of time after the consumer's  
3 receipt of the notice sent by the controller under subsection (6)(b)  
4 of this section.

5 (b) The appeal process must be conspicuously available and as  
6 easy to use as the process for submitting such requests under this  
7 section.

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

22 (d) When informing a consumer of any action taken or not taken in  
23 response to an appeal pursuant to (c) of this subsection, the  
24 controller must clearly and prominently ask the consumer whether the  
25 consumer consents to having the controller submit the appeal, along  
26 with any action taken or not taken by the controller in response to  
27 the appeal and must, upon request, provide the controller's written  
28 explanation of the reasons in support thereof, to the attorney  
29 general. If the consumer provides such consent, the controller must  
30 submit such information to the attorney general.

31 NEW SECTION. **Sec. 7.** PROCESSING DEIDENTIFIED DATA OR  
32 PSEUDONYMOUS DATA. (1) This chapter does not require a controller or  
33 processor to do any of the following solely for purposes of complying  
34 with this chapter:

35 (a) Reidentify deidentified data;

36 (b) Comply with an authenticated consumer request to access,  
37 correct, delete, or port personal data pursuant to section 6 (1)  
38 through (4) of this act, if all of the following are true:

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

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

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

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

16 (2) The rights contained in section 6 (1) through (4) of this act  
17 do not apply to pseudonymous data in cases where the controller is  
18 able to demonstrate any information necessary to identify the  
19 consumer is kept separately and is subject to effective technical and  
20 organizational controls that prevent the controller from accessing  
21 such information.

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

27 NEW SECTION. **Sec. 8.** RESPONSIBILITIES OF CONTROLLERS. (1)

28 *Transparency.*

29 (a) Controllers shall provide consumers with a reasonably  
30 accessible, clear, and meaningful privacy notice that includes:

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

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

34 (iii) How and where consumers may exercise the rights contained  
35 in section 6 of this act, including how a consumer may appeal a  
36 controller's action with regard to the consumer's request;

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

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

3 (b) If a controller sells personal data to third parties or  
4 processes personal data for targeted advertising, it must clearly and  
5 conspicuously disclose such processing, as well as the manner in  
6 which a consumer may exercise the right to opt out of such  
7 processing, in a clear and conspicuous manner.

8 (c) Controllers shall establish, and shall describe in the  
9 privacy notice, one or more secure and reliable means for consumers  
10 to submit a request to exercise their rights under this chapter. Such  
11 means shall take into account the ways in which consumers interact  
12 with the controller, the need for secure and reliable communication  
13 of such requests, and the controller's ability to authenticate the  
14 identity of the consumer making the request. Controllers shall not  
15 require a consumer to create a new account in order to exercise a  
16 right, but a controller may require a consumer to use an existing  
17 account to exercise the consumer's rights under this chapter.

18 (2) *Purpose specification.* A controller's collection of personal  
19 data must be limited to what is reasonably necessary in relation to  
20 the purposes for which such data are processed, as disclosed to the  
21 consumer.

22 (3) *Data minimization.* A controller's collection of personal data  
23 must be only as reasonably necessary to provide services requested by  
24 a consumer, to conduct an activity that a consumer has requested, or  
25 to verify requests made pursuant to section 6 of this act.

26 (4) *Avoid secondary use.* Except as provided in this chapter, a  
27 controller may not process personal data for purposes that are not  
28 reasonably necessary to, or compatible with, the purposes for which  
29 such personal data are processed, as disclosed to the consumer,  
30 unless the controller obtains the consumer's consent.

31 (5) *Security.* A controller shall establish, implement, and  
32 maintain reasonable administrative, technical, and physical data  
33 security practices to protect the confidentiality, integrity, and  
34 accessibility of personal data. Such data security practices shall be  
35 appropriate to the volume and nature of the personal data at issue.

36 (6) *Nondiscrimination.* A controller may not process personal data  
37 in violation of state and federal laws that prohibit unlawful  
38 discrimination against consumers. A controller shall not discriminate  
39 against a consumer for exercising any of the rights contained in this  
40 chapter, including denying goods or services to the consumer,



1 charging different prices or rates for goods or services, and  
2 providing a different level of quality of goods and services to the  
3 consumer. This subsection shall not prohibit a controller from  
4 offering a different price, rate, level, quality, or selection of  
5 goods or services to a consumer, including offering goods or services  
6 for no fee, if the offering is in connection with a consumer's  
7 voluntary participation in a bona fide loyalty, rewards, premium  
8 features, discounts, or club card program. A controller may not sell  
9 personal data to a third-party controller as part of such a program  
10 unless: (a) The sale is reasonably necessary to enable the third  
11 party to provide a benefit to which the consumer is entitled; (b) the  
12 sale of personal data to third parties is clearly disclosed in the  
13 terms of the program; and (c) the third party uses the personal data  
14 only for purposes of facilitating such benefit to which the consumer  
15 is entitled and does not retain or otherwise use or disclose the  
16 personal data for any other purpose. A controller may not enroll a  
17 consumer in a facial recognition service in connection with a bona  
18 fide loyalty, rewards, premium features, discounts, or club card  
19 program.

20 (7) *Sensitive data.* Except as otherwise provided in this act, a  
21 controller may not process sensitive data concerning a consumer  
22 without obtaining the consumer's consent, or, in the case of the  
23 processing of personal data concerning a known child, without  
24 obtaining consent from the child's parent or lawful guardian, in  
25 accordance with the children's online privacy protection act  
26 requirements.

27 (8) *Nonwaiver of consumer rights.* Any provision of a contract or  
28 agreement of any kind that purports to waive or limit in any way a  
29 consumer's rights under this chapter shall be deemed contrary to  
30 public policy and shall be void and unenforceable.

31 NEW SECTION. **Sec. 9.** DATA PROTECTION ASSESSMENTS. (1)  
32 Controllers must conduct and document a data protection assessment of  
33 each of the following processing activities involving personal data:

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

36 (b) The sale of personal data;

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

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

6 (d) The processing of sensitive data; and

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

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

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

24 (3) The attorney general may request, in writing, that a  
25 controller disclose any data protection assessment that is relevant  
26 to an investigation conducted by the attorney general. The controller  
27 must make a data protection assessment available to the attorney  
28 general upon such a request. The attorney general may evaluate the  
29 data protection assessments for compliance with the responsibilities  
30 contained in section 8 of this act and with other laws including, but  
31 not limited to, chapter 19.86 RCW. Data protection assessments are  
32 confidential and exempt from public inspection and copying under  
33 chapter 42.56 RCW. The disclosure of a data protection assessment  
34 pursuant to a request from the attorney general under this subsection  
35 does not constitute a waiver of the attorney-client privilege or work  
36 product protection with respect to the assessment and any information  
37 contained in the assessment.

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

1        NEW SECTION.    **Sec. 10.**    LIMITATIONS AND APPLICABILITY. (1) The

2 obligations imposed on controllers or processors under this chapter  
3 do not restrict a controller's or processor's ability to:

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

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

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

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

15        (e) Provide a product or service specifically requested by a  
16 consumer, perform a contract to which the consumer is a party, or  
17 take steps at the request of the consumer prior to entering into a  
18 contract;

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

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

27        (h) Engage in public or peer-reviewed scientific, historical, or  
28 statistical research in the public interest that adheres to all other  
29 applicable ethics and privacy laws if the deletion of the information  
30 is likely to render impossible or seriously impair the achievement of  
31 the research and the consumer provided consent; or

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

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

37        (a) Conduct internal research solely to improve or repair  
38 products, services, or technology;

39        (b) Identify and repair technical errors that impair existing or  
40 intended functionality; or

1 (c) Perform solely internal operations that are reasonably  
2 aligned with the expectations of the consumer based on the consumer's  
3 existing relationship with the controller, or are otherwise  
4 compatible with processing in furtherance of the provision of a  
5 product or service specifically requested by a consumer or the  
6 performance of a contract to which the consumer is a party.

7 (3) The obligations imposed on controllers or processors under  
8 this chapter do not apply where compliance by the controller or  
9 processor with this chapter would violate an evidentiary privilege  
10 under Washington law and do not prevent a controller or processor  
11 from providing personal data concerning a consumer to a person  
12 covered by an evidentiary privilege under Washington law as part of a  
13 privileged communication.

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

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

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

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

32 (6) Personal data that are processed by a controller pursuant to  
33 this section must not be processed for any purpose other than those  
34 expressly listed in this section. Personal data that are processed by  
35 a controller pursuant to this section may be processed solely to the  
36 extent that such processing is: (i) Necessary, reasonable, and  
37 proportionate to the purposes listed in this section; and (ii)  
38 adequate, relevant, and limited to what is necessary in relation to  
39 the specific purpose or purposes listed in this section. Furthermore,  
40 personal data that are collected, used, or retained pursuant to

1 subsection (2) of this section must, insofar as possible, taking into  
2 account the nature and purpose or purposes of such collection, use,  
3 or retention, be subjected to reasonable administrative, technical,  
4 and physical measures to protect the confidentiality, integrity, and  
5 accessibility of the personal data, and to reduce reasonably  
6 foreseeable risks of harm to consumers relating to such collection,  
7 use, or retention of personal data.

8 (7) If a controller processes personal data pursuant to an  
9 exemption in this section, the controller bears the burden of  
10 demonstrating that such processing qualifies for the exemption and  
11 complies with the requirements in subsection (6) of this section.

12 (8) Processing personal data solely for the purposes expressly  
13 identified in subsection (1)(a) through (d) or (g) of this section  
14 does not, by itself, make an entity a controller with respect to such  
15 processing.

16 NEW SECTION. **Sec. 11.** ENFORCEMENT. (1) The legislature finds  
17 that 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. A violation of this  
20 chapter is not reasonable in relation to the development and  
21 preservation of business and is an unfair or deceptive act in trade  
22 or commerce and an unfair method of competition for the purpose of  
23 applying the consumer protection act, chapter 19.86 RCW.

24 (2) Any controller or processor that violates this chapter is  
25 subject to an injunction and liable for a civil penalty of not more  
26 than seven thousand five hundred dollars for each violation.

27 NEW SECTION. **Sec. 12.** CONSUMER PRIVACY ACCOUNT. The consumer  
28 privacy account is created in the state treasury. All receipts from  
29 the imposition of civil penalties under this chapter must be  
30 deposited into the account except for the recovery of costs and  
31 attorneys' fees accrued by the attorney general in enforcing this  
32 chapter. Moneys in the account may be spent only after appropriation.  
33 Moneys in the account may only be used for the purposes of the office  
34 of privacy and data protection as created under RCW 43.105.369, and  
35 may not be used to supplant general fund appropriations to the  
36 agency.

1        NEW SECTION.    **Sec. 13.**    PREEMPTION. (1) This chapter supersedes  
2 and preempts laws, ordinances, regulations, or the equivalent adopted  
3 by any local entity regarding the processing of personal data by  
4 controllers or processors. Laws, ordinances, or regulations regarding  
5 the processing of personal data by controllers or processors that are  
6 adopted by any local entity prior to the effective date of this  
7 chapter are not superseded or preempted.

8        (2) This chapter does not supersede or preempt laws, ordinances,  
9 regulations, or the equivalent adopted by any local entity regarding  
10 facial recognition.

11        NEW SECTION.    **Sec. 14.**    THE OFFICE OF PRIVACY AND DATA PROTECTION  
12 REPORT. (1) By December 1, 2020, the office of privacy and data  
13 protection shall prepare and post to its public web site a report  
14 that summarizes the data protected and not protected by this chapter.  
15 At a minimum, the report must include, with reasonable detail, a list  
16 of the types of information that are publicly available from local,  
17 state, and federal government sources, and an inventory of  
18 information to which this chapter does not apply by virtue of a  
19 limitation in section 4 of this act. The report may be updated as new  
20 information becomes available to the office.

21        (2) The office of privacy and data protection may consult with  
22 stakeholders and provide recommendations regarding the appropriate  
23 breadth and number of circumstances that limit the obligations of  
24 controllers and processors, and in particular whether those limits  
25 should apply for a prescribed period of time or in perpetuity.

26        (3) The office of privacy and data protection may consult with  
27 stakeholders, including those in the industry, academia, and consumer  
28 and privacy advocacy, regarding the scope and coverage of this  
29 chapter.

30        NEW SECTION.    **Sec. 15.**    ATTORNEY GENERAL REPORT. (1) The attorney  
31 general shall compile a report evaluating the liability and  
32 enforcement provisions of this chapter including, but not limited to,  
33 the effectiveness of its efforts to enforce this chapter, and any  
34 recommendations for changes to such provisions.

35        (2) The attorney general shall submit the report to the governor  
36 and the appropriate committees of the legislature by July 1, 2022.

1        NEW SECTION.    **Sec. 16.**    JOINT RESEARCH INITIATIVES. The governor  
2 may enter into agreements with the governments of the Canadian  
3 province of British Columbia and the states of California and Oregon  
4 for the purpose of sharing personal data or personal information by  
5 public bodies across national and state borders to enable  
6 collaboration for joint data-driven research initiatives. Such  
7 agreements must provide reciprocal protections that the respective  
8 governments agree appropriately safeguard the data.

9        NEW SECTION.    **Sec. 17.**    FACIAL RECOGNITION. (1) Processors that  
10 provide facial recognition services must make available an  
11 application programming interface or other technical capability,  
12 chosen by the processor, to enable controllers or third parties to  
13 conduct legitimate, independent, and reasonable tests of those facial  
14 recognition services for accuracy and unfair performance differences  
15 across distinct subpopulations: PROVIDED, That making such an  
16 application programming interface or other technical capability  
17 available does not require the disclosure of proprietary data, trade  
18 secrets, intellectual property, or other information, or if doing so  
19 would increase the risk of cyberattacks including, without  
20 limitation, cyberattacks related to unique methods of conducting  
21 business, data unique to the product or services, or determining  
22 prices or rates to be charged for services. Such subpopulations are  
23 defined by visually detectable characteristics, such as (a) race,  
24 skin tone, ethnicity, gender, age, or disability status, or (b) other  
25 protected characteristics that are objectively determinable or self-  
26 identified by the individuals portrayed in the testing dataset. If  
27 the results of that independent testing identify material unfair  
28 performance differences across subpopulations and the methodology,  
29 data, and results are disclosed in a manner that allow full  
30 reproduction of the testing directly to the processor, who, acting  
31 reasonably, determines that the methodology and results of that  
32 testing are valid, then the processor must develop and implement a  
33 plan to mitigate the identified performance differences. Nothing in  
34 this subsection prevents a processor from prohibiting the use of the  
35 processor's facial recognition service by a competitor for  
36 competitive purposes.

37        (2) Processors that provide facial recognition services must  
38 provide documentation that includes general information that:

1 (a) Explains the capabilities and limitations of the services in  
2 plain language; and

3 (b) Enables testing of the services in accordance with this  
4 section.

5 (3) Processors that provide facial recognition services must  
6 prohibit, in the contract required by section 5 of this act, the use  
7 of facial recognition services by controllers to unlawfully  
8 discriminate under federal or state law against individual consumers  
9 or groups of consumers.

10 (4) Controllers must provide a conspicuous and contextually  
11 appropriate notice whenever a facial recognition service is deployed  
12 in a physical premise open to the public that includes, at minimum,  
13 the following:

14 (a) The purpose or purposes for which the facial recognition  
15 service is deployed; and

16 (b) Information about where consumers can obtain additional  
17 information about the facial recognition service including, but not  
18 limited to, a link to any applicable online notice, terms, or policy  
19 that provides information about where and how consumers can exercise  
20 any rights that they have with respect to the facial recognition  
21 service.

22 (5) Controllers must obtain consent from a consumer prior to  
23 enrolling an image of that consumer in a facial recognition service  
24 used in a physical premise open to the public.

25 (6) Controllers using a facial recognition service to make  
26 decisions that produce legal effects on consumers or similarly  
27 significant effects on consumers must ensure that those decisions are  
28 subject to meaningful human review.

29 (7) Prior to deploying a facial recognition service in the  
30 context in which it will be used, controllers using a facial  
31 recognition service to make decisions that produce legal effects on  
32 consumers or similarly significant effects on consumers must test the  
33 facial recognition service in operational conditions. Controllers  
34 must take commercially reasonable steps to ensure best quality  
35 results by following all reasonable guidance provided by the  
36 developer of the facial recognition service.

37 (8) Controllers using a facial recognition service must conduct  
38 periodic training of all individuals that operate a facial  
39 recognition service or that process personal data obtained from the



1 use of facial recognition services. Such training shall include, but  
2 not be limited to, coverage of:

3 (a) The capabilities and limitations of the facial recognition  
4 service, including facial recognition rates of error based on  
5 demographical differences among different subpopulations;

6 (b) Procedures to interpret and act on the output of the facial  
7 recognition service; and

8 (c) The meaningful human review requirement for decisions that  
9 produce legal effects on consumers or similarly significant effects  
10 on consumers, to the extent applicable to the deployment context.

11 (9) Controllers shall not knowingly disclose personal data  
12 obtained from a facial recognition service to a law enforcement  
13 agency, except when such disclosure is:

14 (a) Pursuant to the consent of the consumer to whom the personal  
15 data relates;

16 (b) Required by federal, state, or local law in response to a  
17 court-ordered warrant;

18 (c) Necessary to prevent or respond to an emergency involving  
19 danger of death or serious physical injury to any person, upon a good  
20 faith belief by the controller; or

21 (d) To the national center for missing and exploited children, in  
22 connection with a report submitted thereto under Title 18 U.S.C. Sec.  
23 2258A.

24 (10) Controllers that deploy a facial recognition service must  
25 respond to a consumer request to exercise the rights specified in  
26 section 6 of this act and must fulfill the responsibilities  
27 identified in section 8 of this act.

28 (11) Voluntary facial recognition services used to verify an  
29 aviation passenger's identity in connection with services regulated  
30 by the secretary of transportation under Title 49 U.S.C. Sec. 41712  
31 and exempt from state regulation under Title 49 U.S.C. Sec.  
32 41713(b)(1) are exempt from this section. Images captured by an  
33 airline must not be retained for more than twenty-four hours and,  
34 upon request of the attorney general, airlines must certify that they  
35 do not retain the image for more than twenty-four hours. An airline  
36 facial recognition service must disclose and obtain consent from the  
37 customer prior to capturing an image.

1        NEW SECTION.        **Sec. 18.**        This chapter does not apply to  
2 institutions of higher education or nonprofit corporations until July  
3 31, 2024.

4        NEW SECTION.        **Sec. 19.**        Sections 1 through 18 and 20 of this act  
5 constitute a new chapter in Title 19 RCW.

6        NEW SECTION.        **Sec. 20.**        This act takes effect July 31, 2021."

7        Correct the title.

EFFECT: (1) Modifies the jurisdictional scope thresholds to make the requirements of the bill applicable to legal entities that control or process personal data of at least twenty-five thousand consumers and derive over twenty-five, rather than fifty, percent of gross revenue from the sale of personal data.

(2) Provides that controllers must allow guardians or conservators to exercise consumer personal data rights on behalf of consumers subject to guardianship or conservatorship.

(3) Removes provisions related to the private right of action and liability allocation.

(4) Removes provisions giving the Attorney General exclusive enforcement authority and provides that violations are enforceable under the Consumer Protection Act.

(5) Specifies that local laws, ordinances, or regulations regarding the processing of personal data by controllers or processors that are adopted prior to the effective date of the bill are not superseded or preempted.

(6) Specifies that local laws, ordinances, or regulations regarding facial recognition are not preempted.

(7) Modifies the data minimization responsibility of a controller by requiring that the controller's collection of personal data be only as reasonably necessary for specified purposes, rather than adequate, relevant, and limited to what is necessary for processing purposes disclosed to consumer.

(8) Specifies in the definition of "consumer" that acting in an individual or household context includes buying and selling in an individual or household context.

(9) Requires the Office of Privacy and Data Protection (OPDP) to produce a public report regarding the data protected by the bill. Authorizes the OPDP to consult with stakeholders regarding the scope and coverage of the bill, as well as the appropriate breadth and number of circumstances that limit the obligations of controllers and processors.

(10) Specifies that certain transactions do not count as "consumers" for purposes of the thresholds that a legal entity must meet before it is subject to the requirements in the bill.

(11) Removes provisions that permit controllers to enroll a consumer's image in a facial recognition service without first obtaining the consumer's consent.

(12) Requires facial recognition training to include coverage of facial recognition error rates based on demographical differences.

(13) Permits disclosure of personal data obtained from a facial recognition service to law enforcement when required in response to a

court-ordered warrant, rather than a court order, or subpoena or summons issued by a judicial officer or grand jury.

--- **END** ---