

By Representative Kloba

1 Beginning on page 1, after line 2, strike all material through
2 "immediately." on page 46, line 16 and insert the 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 AND INTENT. (1) The
6 legislature finds that the people of Washington regard their privacy
7 as a 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, protect public health associated with
25 global pandemics, and improve quality of life, the legislature seeks
26 to shape responsible public policies where innovation and protection
27 of individual privacy coexist. The legislature notes that our federal
28 authorities have not developed or adopted into law regulatory or
29 legislative solutions that give consumers control over their privacy.
30 In contrast, the European Union's general data protection regulation
31 has continued to influence data privacy policies and practices of

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

6 (4) With this act, the legislature intends to: Provide a modern
7 privacy regulatory framework with data privacy guardrails to protect
8 individual privacy; establish mechanisms for consumers to exercise
9 control over their data; and require companies to be responsible
10 custodians of data as technological innovations emerge.

11 (5) This act gives consumers the ability to protect their own
12 rights to privacy by explicitly providing consumers the right to
13 access, correct, and delete personal data, as well as the rights to
14 obtain data in a portable format. These rights will add to, and not
15 subtract from, the consumer protection rights that consumers already
16 have under Washington state law.

17 (6) This act also imposes affirmative obligations upon companies
18 to safeguard personal data, and provide clear, understandable, and
19 transparent information to consumers about how their personal data is
20 used. It strengthens compliance and accountability by requiring data
21 protection assessments in the collection and use of personal data.
22 Finally, it empowers the state attorney general to obtain and
23 evaluate a company's data protection assessments, to conduct
24 investigations, while preserving consumers' rights under the consumer
25 protection act to impose penalties where violations occur, and to
26 prevent against future violations.

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

30 (1) "Affiliate" means a legal entity that controls, is controlled
31 by, or is under common control with, that other legal entity. For
32 these purposes, "control" or "controlled" means: Ownership of, or the
33 power to vote, more than 50 percent of the outstanding shares of any
34 class of voting security of a company; control in any manner over the
35 election of a majority of the directors or of individuals exercising
36 similar functions; or the power to exercise a controlling influence
37 over the management of a company.

1 (2) "Air carriers" has the same meaning as defined in the federal
2 aviation act (49 U.S.C. Sec. 40101, et seq.), including the airline
3 deregulation act (49 U.S.C. 41713).

4 (3) "Authenticate" means to use reasonable means to determine
5 that a request to exercise any of the rights in section 104 (1)
6 through (4) of this act is being made by the consumer who is entitled
7 to exercise such rights with respect to the personal data at issue.

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

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

36 (6) "Child" has the same meaning as defined in the children's
37 online privacy protection act, Title 15 U.S.C. Sec. 6501 through
38 6506.

39 (7) "Consent" means any freely given, specific, informed, and
40 unambiguous indication of the consumer's wishes by which the consumer

1 signifies agreement to the processing of personal data relating to
2 the consumer for a narrowly defined particular purpose. Acceptance of
3 a general or broad terms of use or similar document that contains
4 descriptions of personal data processing along with other, unrelated
5 information, does not constitute consent. Hovering over, muting,
6 pausing, or closing a given piece of content does not constitute
7 consent. Likewise, agreement obtained through dark patterns does not
8 constitute consent.

9 (8) "Consumer" means a natural person who is a Washington
10 resident acting only in an individual or household context. It does
11 not include a natural person acting in a commercial or employment
12 context.

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

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

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

22 (12) "Decisions that produce legal effects concerning a consumer
23 or similarly significant effects concerning a consumer" means
24 decisions that result in the provision or denial of financial and
25 lending services, housing, insurance, education enrollment, criminal
26 justice, employment opportunities, health care services, or access to
27 basic necessities, such as food and water.

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

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

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

3 (15) "Harm" means any potential or realized adverse consequences
4 to a consumer or to society, including but not limited to:

5 (a) Direct or indirect financial harm;

6 (b) Physical harm or threats to consumers or property, including
7 but not limited to bias-related crimes and threats, harassment, and
8 sexual harassment;

9 (c) Discrimination in products, services, or economic
10 opportunity, such as housing, employment, credit, insurance,
11 education, or health care, on the basis of a consumer's or class of
12 consumers' actual or perceived age, race, national origin, sex,
13 sexual orientation, gender identity, disability, and/or membership in
14 another protected class, except as specifically authorized by law;

15 (d) Interference with or surveillance of First Amendment
16 protected activities by state actors, except as specifically
17 authorized by law;

18 (e) Interference with the right to vote or with free and fair
19 elections;

20 (f) Violation of consumers' rights to due process or equal
21 protection under the law;

22 (g) Loss of individual control over personal data via
23 nonconsensual sharing of private information, data breach, or other
24 actions that violate the rights listed in section 104 of this act;

25 (h) The nonconsensual capture of information or communications
26 within a consumer's home or where the consumer is entitled to have a
27 reasonable expectation of privacy or access control; and

28 (i) Other effects on a consumer that may not be reasonably
29 foreseeable to, contemplated by, or expected by the consumer to whom
30 the personal data relates, that are nevertheless reasonably
31 foreseeable, contemplated by, or expected by the controller, and that
32 alter or limit that consumer's choices or predetermines results.

33 (16) "Health care facility" has the same meaning as defined in
34 RCW 70.02.010.

35 (17) "Health care information" has the same meaning as defined in
36 RCW 70.02.010.

37 (18) "Health care provider" has the same meaning as defined in
38 RCW 70.02.010.

39 (19) "Identified or identifiable natural person" means a person
40 who can be readily identified, directly or indirectly.

1 (20) "Institutions of higher education" has the same meaning as
2 in RCW 28B.92.030.

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

5 (22) "Known child" means a child under circumstances where a
6 controller has actual knowledge of, or willfully disregards, the
7 child's age.

8 (23) "Legislative agencies" has the same meaning as defined in
9 RCW 44.80.020.

10 (24) "Local government" has the same meaning as in RCW 39.46.020.

11 (25) "Minor" means an individual who is at least 13 and under 16
12 years of age under circumstances where a controller has actual
13 knowledge of, or willfully disregards, the minor's age.

14 (26) "Monetize" means to sell, rent, release, disclose,
15 disseminate, trade, make available, transfer, or otherwise
16 communicate orally, in writing, or by electronic or other means, a
17 consumer's personal data by a controller, processor, or a third party
18 in exchange for monetary or other consideration, as well as to
19 leverage or use a consumer's personal data to place a targeted
20 advertisement or to otherwise profit, regardless of whether the
21 consumer's personal data changes hands.

22 (27) "Nonprofit corporation" has the same meaning as in RCW
23 24.03.005.

24 (28) "Personal data" means any information, including
25 pseudonymous data, that is linked or reasonably linkable to an
26 identified or identifiable natural person who is a Washington
27 resident and that is captured in an interaction in which a controller
28 directly or indirectly makes available information, products, or
29 services to a consumer or household. Covered interactions include but
30 are not limited to posting of information, offering of a product or
31 service, the placement of targeted advertisements, or offering a
32 membership or other ongoing relationship with an entity. For the
33 purposes of this chapter, "personal data" includes biometric
34 information, regardless of how captured.

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

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

3 (31) "Profiling" means any form of automated processing of
4 personal data to evaluate, analyze, or predict personal aspects
5 concerning an identified or identifiable natural person's economic
6 situation, health, personal preferences, interests, reliability,
7 behavior, location, or movements.

8 (32) "Protected health information" has the same meaning as
9 defined in Title 45 C.F.R., established pursuant to the federal
10 health insurance portability and accountability act of 1996.

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

17 (34) "Publicly available information" means information that is
18 lawfully made available from federal, state, or local government
19 records.

20 (35)(a) "Sale," "sell," or "sold" means the exchange of personal
21 data for monetary or other valuable consideration by the controller
22 to a third party or to otherwise profit, regardless of whether the
23 consumer's personal data changes hands.

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

37 (36) "Sensitive data" means (a) personal data revealing racial or
38 ethnic origin, religious beliefs, mental or physical health condition
39 or diagnosis, sexual orientation, or citizenship or immigration
40 status; (b) the processing of genetic or biometric data for the

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

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

11 (38) "State agency" has the same meaning as in RCW 43.105.020.

12 (39) "Targeted advertising" means displaying advertisements to a
13 consumer where the advertisement is selected based on personal data
14 obtained from a consumer's activities over time and across one or
15 more distinctly branded websites or online applications to predict
16 the consumer's preferences or interests. It does not include
17 advertising: (a) Based on activities within a controller's own
18 commonly branded websites or online applications; (b) based on the
19 context of a consumer's current search query or visit to a website or
20 online application; or (c) to a consumer in response to the
21 consumer's request for information or feedback.

22 (40) "Third party" means a natural or legal person, public
23 authority, agency, or body other than the consumer, controller,
24 processor, or an affiliate of the processor or the controller.

25 (41) "Washington governmental entity" means a department or
26 agency of Washington state or a political subdivision thereof,
27 including but not limited to public authorities and special use
28 districts, or an individual acting for or on behalf of the state or a
29 political subdivision thereof.

30 NEW SECTION. **Sec. 102.** JURISDICTIONAL SCOPE. (1) This chapter
31 applies to legal entities that conduct business in Washington or
32 produce products or services that are targeted to residents of
33 Washington, and that satisfy one or more of the following thresholds:

34 (a) During a calendar year, processes the personal data of 1,000
35 or more unique consumers; or

36 (b) Processes personal data and earns or receives \$10,000,000 or
37 more of annual revenue through 300 or more transactions.

38 (2) This chapter does not apply to:

1 (a) State agencies, legislative agencies, the judicial branch,
2 local governments, or tribes, except as provided in sections 108 and
3 113 of this act;

4 (b) Municipal corporations, except as provided in sections 108
5 and 113 of this act;

6 (c) Air carriers;

7 (d) Nonprofit organizations that:

8 (i) Are registered with the secretary of state under the
9 charities program pursuant to chapter 19.09 RCW;

10 (ii) Collect personal data during legitimate activities related
11 to the organization's tax-exempt purpose; and

12 (iii) Do not sell personal data collected by the organization;

13 (e) Information that meets the definition of:

14 (i) Protected health information for purposes of the federal
15 health insurance portability and accountability act of 1996 and
16 related regulations;

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

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

20 (iv) Identifiable private information for purposes of the federal
21 policy for the protection of human subjects, 45 C.F.R. Part 46;
22 identifiable private information that is otherwise information
23 collected as part of human subjects research pursuant to the good
24 clinical practice guidelines issued by the international council for
25 harmonization; the protection of human subjects under 21 C.F.R. Parts
26 50 and 56; or personal data used or shared in research conducted in
27 accordance with one or more of the requirements set forth in this
28 subsection;

29 (v) Information and documents created specifically for, and
30 collected and maintained by:

31 (A) A quality improvement committee for purposes of RCW
32 43.70.510, 70.230.080, or 70.41.200;

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

34 (C) A quality assurance committee for purposes of RCW 74.42.640
35 or 18.20.390;

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

1 (vi) Information and documents created for purposes of the
2 federal health care quality improvement act of 1986, and related
3 regulations;

4 (vii) Patient safety work product for purposes of 42 C.F.R. Part
5 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

6 (viii) Information that is (A) deidentified in accordance with
7 the requirements for deidentification set forth in 45 C.F.R. Part
8 164, and (B) derived from any of the health care-related information
9 listed in this subsection (2)(e);

10 (f) Information originating from, and intermingled to be
11 indistinguishable with, information under (e) of this subsection that
12 is maintained by:

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

16 (ii) A health care facility or health care provider as defined in
17 RCW 70.02.010; or

18 (iii) A program or a qualified service organization as defined by
19 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

20 (g) Information used only for public health activities and
21 purposes as described in 45 C.F.R. Sec. 164.512;

22 (h)(i) An activity involving the collection, maintenance,
23 disclosure, sale, communication, or use of any personal data bearing
24 on a consumer's credit worthiness, credit standing, credit capacity,
25 character, general reputation, personal characteristics, or mode of
26 living by a consumer reporting agency, as defined in Title 15 U.S.C.
27 Sec. 1681a(f), by a furnisher of information, as set forth in Title
28 15 U.S.C. Sec. 1681s-2, who provides information for use in a
29 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by
30 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.
31 1681b.

32 (ii) (h)(i) of this subsection applies only to the extent that
33 such an activity involving the collection, maintenance, disclosure,
34 sale, communication, or use of such personal data by that agency,
35 furnisher, or user is subject to regulation under the fair credit
36 reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the personal
37 data is not collected, maintained, used, communicated, disclosed, or
38 sold except as authorized by the fair credit reporting act;

39 (i) Personal data collected and maintained for purposes of
40 chapter 43.71 RCW;

1 (j) Personal data collected, processed, sold, or disclosed
2 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and
3 implementing regulations, if the collection, processing, sale, or
4 disclosure is in compliance with that law;

5 (k) Personal data collected, processed, sold, or disclosed
6 pursuant to the federal driver's privacy protection act of 1994 (18
7 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or
8 disclosure is in compliance with that law;

9 (l) Personal data regulated by the federal family education
10 rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing
11 regulations;

12 (m) Personal data regulated by the student user privacy in
13 education rights act, chapter 28A.604 RCW;

14 (n) Personal data collected, maintained, disclosed, or otherwise
15 used in connection with the gathering, dissemination, or reporting of
16 news or information to the public by news media as defined in RCW
17 5.68.010(5);

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

23 (p) Data collected or maintained: (i) In the course of an
24 individual acting as a job applicant to, an employee of, owner of,
25 director of, officer of, medical staff member of, or contractor of
26 that business to the extent that it is collected and used solely
27 within the context of that role; (ii) as the emergency contact
28 information of an individual under (p)(i) of this subsection used
29 solely for emergency contact purposes; or (iii) that is necessary for
30 the business to retain to administer benefits for another individual
31 relating to the individual under (p)(i) of this subsection is used
32 solely for the purposes of administering those benefits.

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

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

1 NEW SECTION. **Sec. 103.** OPT-IN CONSENT. (1) A controller may
2 not, without freely given, specific, informed, and unambiguous opt-in
3 consent from a consumer:

4 (a) Process the consumers personal data; or

5 (b) Make any changes in the processing of the consumer's personal
6 data that would necessitate a change to the privacy notice required
7 to be provided under section 110 of this act.

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

12 (3) A controller requesting consent shall ensure that the option
13 to withhold consent is presented as clearly and prominently as the
14 option to provide consent.

15 (4) A controller shall provide a mechanism for a consumer to
16 withdraw previously given consent at any time. The consumer must be
17 notified when the withdrawal of consent is complete. It must be as
18 easy for a consumer to withdraw consent as it is to provide consent.

19 (5) Under no circumstances shall a consumer's interaction with a
20 controller's product or service when the controller has a terms of
21 service or a privacy policy in and of itself constitute freely given,
22 specific, informed, and unambiguous consent.

23 (6) To the extent that a controller must process internet
24 protocol addresses, system configuration information, uniform
25 resource locators of referring pages, locale and language
26 preferences, keystrokes, and other personal data in order to obtain a
27 consumer's freely given, specific, informed, and unambiguous opt-in
28 consent, the controller shall:

29 (a) Process only the personal data necessary to request freely
30 given, specific, informed, and unambiguous opt-in consent;

31 (b) Process the personal data solely to request freely given,
32 specific, informed, and unambiguous opt-in consent; and

33 (c) Immediately delete the personal data if consent is not given.

34 (7) A controller shall not refuse to serve a consumer who does
35 not approve the processing of the consumer's personal data under this
36 section unless the processing is necessary for the primary purpose of
37 the transaction that the consumer has requested.

38 (8) A controller shall not discriminate against consumers by
39 reason of their not granting opt-in consent to the processing of
40 their personal data under this chapter or otherwise exercising their

1 rights under this chapter, including but not limited to, by: Denying
2 goods or services to the consumer; charging different prices or rates
3 for goods or services, including through the use of discounts or
4 other benefits or imposing penalties; providing a different level or
5 quality of goods or services to the consumer; and suggesting that the
6 consumer will receive a different price or rate for goods or services
7 or a different level or quality of goods or services. Notwithstanding
8 this subsection, a controller may, with the consumer's opt-in consent
9 given in compliance with this section, operate a program in which
10 information, products, or services sold to the consumer are
11 discounted based on that consumer's prior purchases from the
12 controller, provided that the personal data shall be processed solely
13 for the purpose of operating such program.

14 (9) A controller shall not state or imply that the quality of a
15 product or service will be diminished and shall not actually diminish
16 the quality of a product or service if the consumer declines to give
17 opt-in consent to personal data processing.

18 (10) The Washington state department of commerce is hereby
19 authorized and directed to conduct a study to determine the most
20 effective way for controllers to obtain the consumers' freely given,
21 specific, informed, and unambiguous opt-in consent for each type of
22 personal data processing. The Washington state department of commerce
23 may request data and information from controllers conducting business
24 in Washington state, other Washington state government entities
25 administering notice and consent regimes, consumer protection
26 experts, privacy advocates, researchers, internet standards setting
27 bodies such as the internet engineering task force and institute of
28 electrical and electronics engineers, and other relevant sources to
29 meet the purpose of the study.

30 (11) Within six months of enactment of this act, the Washington
31 state department of commerce shall adopt regulations specifying how:

32 (a) Controllers must notify consumers of their rights under this
33 chapter and obtain the consumers' freely given, specific, informed,
34 and unambiguous opt-in consent for each use model of personal data
35 processing; and

36 (b) Controllers must notify consumers of their right to withdraw
37 their consent at any time and how the right may be exercised.

38 (12) Within six months of enactment of this act, the Washington
39 state department of commerce shall adopt regulations grouping
40 different types of processing of personal data by use model and

1 permitting a controller to simultaneously obtain freely given,
2 specific, informed, and unambiguous opt-in consent from a consumer
3 for multiple transactions of the same use model.

4 NEW SECTION. **Sec. 104.** CONSUMER RIGHTS. (1) A consumer has the
5 right to confirm whether or not a controller is processing personal
6 data concerning the consumer and access the personal data the
7 controller is processing.

8 (2) A consumer has the right to correct inaccurate personal data
9 concerning the consumer.

10 (3) A consumer has the right to delete personal data concerning
11 the consumer.

12 (4) A consumer has the right to obtain personal data concerning
13 the consumer, which the consumer previously provided to the
14 controller, in a portable and, to the extent technically feasible,
15 readily usable format that allows the individual to transmit the data
16 to another controller without hindrance, where the processing is
17 carried out by automated means.

18 (5) A consumer has the right to refuse consent for any processing
19 of the consumer's personal data that is not essential to the primary
20 transaction.

21 NEW SECTION. **Sec. 105.** EXERCISING CONSUMER RIGHTS. (1) A
22 consumer may exercise the rights set forth in section 104 of this act
23 by submitting a request, at any time, to a controller specifying
24 which rights the consumer wishes to exercise.

25 (2) In the case of processing personal data of a known child, the
26 parent or legal guardian of the known child may exercise the rights
27 of this chapter on the child's behalf.

28 (3) In the case of processing personal data concerning a consumer
29 subject to guardianship, conservatorship, or other protective
30 arrangement under chapter 11.88, 11.92, or 11.130 RCW, the guardian
31 or the conservator of the consumer may exercise the rights of this
32 chapter on the consumer's behalf.

33 NEW SECTION. **Sec. 106.** RESPONDING TO REQUESTS. (1) Except as
34 provided in this chapter, the controller must comply with a request
35 to exercise the rights pursuant to section 104 of this act.

36 (2) (a) Controllers must provide one or more secure and reliable
37 means for consumers to submit a request to exercise their rights

1 under this chapter. These means must take into account the ways in
2 which consumers interact with the controller and the need for secure
3 and reliable communication of the requests.

4 (b) Controllers may not require a consumer to create a new
5 account in order to exercise a right, but a controller may require a
6 consumer to use an existing account to exercise the consumer's rights
7 under this chapter.

8 (3) (a) A controller must inform a consumer of any action taken on
9 a request to exercise any of the rights in section 104 (1) through
10 (4) of this act without undue delay and in any event within 45 days
11 of receipt of the request. That period may be extended once by 45
12 additional days where reasonably necessary, taking into account the
13 complexity and number of the requests. The controller must inform the
14 consumer of any such extension within 45 days of receipt of the
15 request, together with the reasons for the delay.

16 (b) If a controller does not take action on the request of a
17 consumer, the controller must inform the consumer without undue delay
18 and at the latest within 45 days of receipt of the request of the
19 reasons for not taking action and instructions for how to appeal the
20 decision with the controller as described in subsection (4) of this
21 section.

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

30 (d) A controller is not required to comply with a request to
31 exercise any of the rights under section 104 (1) through (4) of this
32 act if the controller is unable to authenticate the request using
33 commercially reasonable efforts. In such a case, the controller may
34 request the provision of additional information reasonably necessary
35 to authenticate the request.

36 (4) (a) A controller must establish an internal process whereby a
37 consumer may appeal a refusal to take action on a request to exercise
38 any of the rights under section 104 of this act within a reasonable
39 period of time after the controller refuses to take action on such
40 request.

1 (b) The appeal process must be conspicuously available and as
2 easy to use as the process for submitting such a request under this
3 section.

4 (c) Within 30 days of receipt of an appeal, a controller must
5 inform the consumer of any action taken or not taken in response to
6 the appeal, along with a written explanation of the reasons in
7 support thereof. That period may be extended by 60 additional days
8 where reasonably necessary, taking into account the complexity and
9 number of the requests serving as the basis for the appeal. The
10 controller must inform the consumer of such an extension within 30
11 days of receipt of the appeal, together with the reasons for the
12 delay. The controller must also provide the consumer with an email
13 address or other online mechanism through which the consumer may
14 submit the appeal, along with any action taken or not taken by the
15 controller in response to the appeal and the controller's written
16 explanation of the reasons in support thereof, to the attorney
17 general.

18 (d) When informing a consumer of any action taken or not taken in
19 response to an appeal pursuant to (c) of this subsection, the
20 controller must clearly and prominently provide the consumer with
21 information about how to file a complaint with the consumer
22 protection division of the attorney general's office. The controller
23 must maintain records of all such appeals and how it responded to
24 them for at least 24 months and shall, upon request, compile and
25 provide a copy of such records to the attorney general.

26 NEW SECTION. **Sec. 107.** SURREPTITIOUS SURVEILLANCE. (1) A
27 consumer has the right to not be subject to surreptitious
28 surveillance.

29 (2) A controller may not activate the microphone, camera, or any
30 other sensor on a device in the lawful possession of a consumer that
31 is capable of collecting or transmitting personal data, without
32 providing the privacy notice required in section 110 of this act and
33 obtaining the consumer's freely given, specific, informed, and
34 unambiguous opt-in consent pursuant to section 103 of this act for
35 the specific type of measurement to be activated; provided that such
36 opt-in consent shall be effective for no more than 90 days after
37 which it shall expire unless renewed by the consumer's freely given,
38 specific, informed, and unambiguous opt-in consent pursuant to
39 section 103 of this act.

1 NEW SECTION. **Sec. 108.** BIOMETRIC INFORMATION. In addition to
2 all provisions of this chapter applicable to personal data, the
3 following provisions are applicable to all biometric information,
4 regardless of how such biometric information is processed.

5 (1) Retention; disclosure; destruction. A controller or
6 Washington governmental entity that processes biometric information
7 must develop a written policy, made available to the public,
8 establishing a retention schedule and guidelines for permanently
9 destroying biometric information when the initial purpose for
10 processing such information has been satisfied or within one year of
11 the consumer's last interaction with the controller or Washington
12 governmental entity, whichever occurs first. Consent under subsection
13 (2) of this section shall be for a period specified in the written
14 consent of not more than one year, and shall automatically expire at
15 the end of such period unless renewed pursuant to subsection (2) of
16 this section. Upon expiration of consent, any biometric information
17 possessed by a controller or Washington governmental entity must be
18 destroyed. Absent a valid warrant issued by a court of competent
19 jurisdiction, a controller or Washington governmental entity in
20 possession of biometric information must comply with its established
21 retention schedule and destruction guidelines.

22 (2) Processing. A controller or Washington governmental entity
23 may not process a consumer's biometric information, unless it first:

24 (a) Informs the consumer in writing that biometric information is
25 being processed;

26 (b) Informs the consumer in writing the details of the specific
27 purpose or purposes and length of term for which biometric
28 information is processed; and

29 (c) Receives a freely given, specific, informed, and unambiguous
30 written opt-in consent executed by the consumer specifically
31 authorizing such processing.

32 (3) Disclosure. No controller or Washington governmental entity
33 in possession of biometric information may disclose or otherwise
34 disseminate a consumer's biometric information unless:

35 (a) The consumer gives freely given, specific, informed, and
36 unambiguous opt-in consent in writing to the disclosure or
37 redisclosure;

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

1 (c) The disclosure or redisclosure is required by state or
2 federal law; or

3 (d) The disclosure is required pursuant to a valid warrant or
4 subpoena issued by a court of competent jurisdiction or a subpoena
5 issued by a governmental entity or in a pending judicial case,
6 provided that in the case of a subpoena the entity subject to the
7 subpoena shall postpone compliance therewith until it has given the
8 subject of the subpoena notice of the facts set forth in section
9 113(2)(b)(i) of this act and has allowed at least 10 business days
10 for the subject to seek review of or otherwise challenge the
11 subpoena.

12 (4) Monetizing. A controller or Washington governmental entity in
13 possession of biometric information may not monetize, or otherwise
14 profit from a consumer's biometric information; provided only that a
15 controller may process a consumer's biometric information, with full
16 disclosure and opt-in consent consistent with section 103 of this
17 act, in a service in which the controller reports to the consumer the
18 biometric information processed or utilizes the biometric information
19 to design or recommend actions or products that have been
20 specifically requested by the consumer with full disclosure that such
21 recommendation is based on the biometric information processed,
22 provided that the biometric information shall not be used for any
23 other purpose.

24 (5) Identification. Notwithstanding any other provision of this
25 chapter, a controller or Washington governmental entity may list
26 personal data such as name or birthdate and biometric information
27 such as height, weight, or photograph on an issued license or
28 membership or identification card for the sole purpose of allowing an
29 employee or other representative of the controller or Washington
30 governmental entity to determine based solely on personal
31 observation, and without the assistance of technologies such as
32 facial recognition, whether the person physically holding such
33 license or card is the person entitled to hold it, provided further
34 that such intended use is disclosed to the consumer prior to
35 capturing the biometric information. Any other processing of such
36 biometric information shall be subject to all the terms and
37 conditions of this chapter. Any controller or governmental entity
38 using personal information or biometric information under this
39 subsection must ensure that it is not stored or processed in any

1 manner that would allow a third party to process such information for
2 any purpose.

3 (6) Consent to processing information pursuant to the protocols
4 for human experimentation constitutes freely given, specific,
5 informed, and unambiguous opt-in consent under this section.

6 NEW SECTION. **Sec. 109.** RESPONSIBILITY ACCORDING TO ROLE. (1)
7 Controllers and processors are responsible for meeting their
8 respective obligations established under this chapter.

9 (2) Processors are responsible under this chapter for adhering to
10 the instructions of the controller and assisting the controller to
11 meet its obligations under this chapter. This assistance includes the
12 following:

13 (a) Taking into account the nature of the processing, the
14 processor shall assist the controller by appropriate technical and
15 organizational measures, insofar as this is possible, for the
16 fulfillment of the controller's obligation to respond to consumer
17 requests to exercise their rights pursuant to section 104 of this
18 act; and

19 (b) Taking into account the nature of processing and the
20 information available to the processor, the processor shall: Assist
21 the controller in meeting the controller's obligations in relation to
22 the security of processing the personal data and in relation to the
23 notification of a breach of the security of the system pursuant to
24 RCW 19.255.010; and provide information to the controller necessary
25 to enable the controller to conduct and document any data protection
26 assessments required by section 112 of this act. The controller and
27 processor are each responsible for only the measures allocated to
28 them.

29 (3) Notwithstanding the instructions of the controller, a
30 processor shall:

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

33 (b) Engage a subcontractor only after providing the controller
34 with an opportunity to object and pursuant to a written contract in
35 accordance with subsection (5) of this section that requires the
36 subcontractor to meet the obligations of the processor with respect
37 to the personal data.

38 (4) Taking into account the context of processing, the controller
39 and the processor shall implement appropriate technical and

1 organizational measures to ensure a level of security appropriate to
2 the risk and establish a clear allocation of the responsibilities
3 between them to implement such measures.

4 (5) Processing by a processor must be governed by a contract
5 between the controller and the processor that is binding on both
6 parties and that sets out the processing instructions to which the
7 processor is bound, including the nature and purpose of the
8 processing, the type of personal data subject to the processing, the
9 duration of the processing, and the obligations and rights of both
10 parties. In addition, the contract must include the requirements
11 imposed by this subsection and subsections (3) and (4) of this
12 section, as well as the following requirements:

13 (a) At the choice of the controller, the processor shall delete
14 or return all personal data to the controller as requested at the end
15 of the provision of services, unless retention of the personal data
16 is required by law;

17 (b) (i) The processor shall make available to the controller all
18 information necessary to demonstrate compliance with the obligations
19 in this chapter; and

20 (ii) The processor shall allow for, and contribute to, reasonable
21 audits and inspections by the controller or the controller's
22 designated auditor. Alternatively, the processor may, with the
23 controller's consent, arrange for a qualified and independent auditor
24 to conduct, at least annually and at the processor's expense, an
25 audit of the processor's policies and technical and organizational
26 measures in support of the obligations under this chapter using an
27 appropriate and accepted control standard or framework and audit
28 procedure for the audits as applicable, and provide a report of the
29 audit to the controller upon request.

30 (6) In no event may any contract relieve a controller or a
31 processor from the liabilities imposed on them by virtue of its role
32 in the processing relationship as defined by this chapter.

33 (7) Determining whether a person is acting as a controller or
34 processor with respect to a specific processing of data is a fact-
35 based determination that depends upon the context in which personal
36 data are to be processed. A person that is not limited in its
37 processing of personal data pursuant to a controller's instructions,
38 or that fails to adhere to such instructions, is a controller and not
39 a processor with respect to a specific processing of data. A
40 processor that continues to adhere to a controller's instructions

1 with respect to a specific processing of personal data remains a
2 processor. If a processor begins, alone or jointly with others,
3 determining the purposes and means of the processing of personal
4 data, it is a controller with respect to the processing.

5 NEW SECTION. **Sec. 110.** RESPONSIBILITIES OF CONTROLLERS. (1) (a)
6 Controllers shall provide consumers with a reasonably accessible,
7 clear, and meaningful privacy notice that includes:

- 8 (i) The categories of personal data processed by the controller;
- 9 (ii) The purposes for which the categories of personal data are
10 processed;
- 11 (iii) How and where consumers may exercise the rights contained
12 in section 104 of this act, including how a consumer may appeal a
13 controller's action with regard to the consumer's request;
- 14 (iv) The categories of personal data that the controller shares
15 with third parties, if any; and
- 16 (v) The categories of third parties, if any, with whom the
17 controller shares personal data.

18 (b) If a controller sells personal data to third parties or
19 processes personal data for targeted advertising, the controller must
20 clearly and conspicuously disclose the processing.

- 21 (c) The privacy notice required under this subsection must:
- 22 (i) Use clear and plain language;
 - 23 (ii) Be in English and any other language in which a controller
24 communicates with the consumer to whom the information pertains; and
 - 25 (iii) Be understandable to the least sophisticated consumer.

26 (2) A controller's collection of personal data must be limited to
27 what is reasonably necessary in relation to the purposes for which
28 the data is processed.

29 (3) A controller's collection of personal data must be adequate,
30 relevant, and limited to what is reasonably necessary in relation to
31 the purposes for which the data is processed.

32 (4) Except as provided in this chapter, a controller may not
33 process personal data for purposes that are not reasonably necessary
34 to, or compatible with, the purposes for which the personal data is
35 processed unless the controller obtains the consumer's consent.

36 (5) A controller shall establish, implement, and maintain
37 reasonable administrative, technical, and physical data security
38 practices to protect the confidentiality, integrity, and

1 accessibility of personal data. The data security practices must be
2 appropriate to the volume and nature of the personal data at issue.

3 (6) A controller shall not process personal data on the basis of
4 a consumer's or a class of consumers' actual or perceived race,
5 color, ethnicity, religion, national origin, sex, gender, gender
6 identity, sexual orientation, familial status, lawful source of
7 income, or disability, in a manner that unlawfully discriminates
8 against the consumer or class of consumers with respect to the
9 offering or provision of: (a) Housing; (b) employment; (c) credit;
10 (d) education; or (e) the goods, services, facilities, privileges,
11 advantages, or accommodations of any place of public accommodation.

12 (7) A controller may not discriminate against a consumer for
13 exercising any of the rights contained in this chapter, including
14 denying goods or services to the consumer, charging different prices
15 or rates for goods or services, and providing a different level of
16 quality of goods and services to the consumer. This subsection does
17 not prohibit a controller from offering a different price, rate,
18 level, quality, or selection of goods or services to a consumer,
19 including offering goods or services for no fee, if the offering is
20 in connection with a consumer's voluntary participation in a bona
21 fide loyalty, rewards, premium features, discounts, or club card
22 program. A controller may not sell personal data to a third-party
23 controller as part of such a program unless: (a) The sale is
24 reasonably necessary to enable the third party to provide a benefit
25 to which the consumer is entitled; (b) the sale of personal data to
26 third parties is clearly disclosed in the terms of the program; and
27 (c) the third party uses the personal data only for purposes of
28 facilitating such a benefit to which the consumer is entitled and
29 does not retain or otherwise use or disclose the personal data for
30 any other purpose.

31 (8) Any provision of a contract or agreement of any kind that
32 purports to waive or limit in any way a consumer's rights under this
33 chapter is deemed contrary to public policy and is void and
34 unenforceable.

35 NEW SECTION. **Sec. 111.** PROCESSING DEIDENTIFIED DATA OR
36 PSEUDONYMOUS DATA. (1) This chapter does not require a controller or
37 processor to do any of the following solely for purposes of complying
38 with this chapter:

39 (a) Reidentify deidentified data;

1 (b) Comply with an authenticated consumer request to access,
2 correct, delete, or port personal data pursuant to section 104 (1)
3 through (4) of this act, if all of the following are true:

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

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

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

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

19 (2) The rights contained in section 104 of this act do not apply
20 to pseudonymous data in cases where the controller is able to
21 demonstrate any information necessary to identify the consumer is
22 kept separately and is subject to effective technical and
23 organizational controls that prevent the controller from accessing
24 such information.

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

30 NEW SECTION. **Sec. 112.** DATA PROTECTION ASSESSMENTS. (1)

31 Controllers must conduct and document a data protection assessment of
32 each of the following processing activities involving personal data:

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

35 (b) The processing of personal data for the purposes of the sale
36 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 110 of this act and, if it serves a civil
31 investigative demand, with RCW 19.86.110. Data protection assessments
32 are 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 unless otherwise subject to case law
38 regarding the applicability of attorney-client privilege or work
39 product protections.

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

4 NEW SECTION. **Sec. 113.** EXCEPTIONS TO THE CONSENT REQUIREMENT.

5 (1) With respect to personal data that is not biometric information,
6 a controller is not required to obtain freely given, specific,
7 informed, and unambiguous opt-in consent from a consumer under
8 section 103 of this act if the processing is necessary to execute the
9 specific transaction for which the consumer is providing personal
10 data, such as the provision of financial information to complete a
11 purchase or the provision of a mailing address to deliver a package.
12 However, personal data shall not be processed for any other purpose
13 beyond that clear primary purpose without the freely given, specific,
14 informed, and unambiguous opt-in consent from the consumer to whom
15 the personal data pertains, except as required by law.

16 (2) With respect to personal data generally, a controller or
17 Washington governmental entity is not required to obtain freely
18 given, specific, informed, and unambiguous opt-in consent from a
19 consumer under section 103 or 108(1) of this act if:

20 (a) It believes that an emergency involving immediate danger of
21 death or serious physical injury to any consumer requires obtaining
22 without delay personal data related to the emergency and the request
23 is narrowly tailored to address the emergency, subject to the
24 following limitations:

25 (i) The request shall document the factual basis for believing
26 that an emergency involving immediate danger of death or serious
27 physical injury to a consumer requires obtaining without delay
28 personal data relating to the emergency; and

29 (ii) Simultaneous with the controller or Washington governmental
30 entity obtaining personal data under this subsection (2)(a), the
31 controller or Washington governmental entity shall use reasonable
32 efforts to inform the consumer of the personal data obtained; the
33 details of the emergency; and the reasons why the controller or
34 Washington governmental entity needed to use, access, or disclose the
35 biometric information and shall continue such efforts to inform until
36 receipt of information is confirmed; and

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

1 (i) Unless a delayed notice is ordered, both the entity
2 requesting the warrant or subpoena and any entity receiving such
3 warrant or subpoena shall, simultaneous with requesting or receiving
4 a warrant compelling disclosure of or serving or receiving a subpoena
5 for personal data, serve or deliver the following information to the
6 subject of the warrant or subpoena by registered or first-class mail,
7 email, or other means reasonably calculated to be effective:

8 (A) A copy of the warrant or subpoena and notice that informs the
9 consumer of the nature of the inquiry with reasonable specificity;

10 (B) That personal data maintained for the consumer was supplied
11 to or requested by the requesting entity and the date on which the
12 supplying or request took place;

13 (C) An inventory of the personal data requested or supplied; and

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

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

25 (iii) In the case of a subpoena, a controller subject to a
26 subpoena shall postpone compliance therewith until it has given the
27 subject of the subpoena notice of the information required under
28 (b)(i) of this subsection and has allowed at least 10 business days
29 for the subject to seek review of or otherwise challenge the
30 subpoena;

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

32 (d) Processing involves only deidentified information.

33 (3) This chapter shall not apply to personal data captured from a
34 patient by a health care provider or health care facility as defined
35 in RCW 48.41.030 or biometric information collected, used, or stored
36 exclusively for medical education or research, public health or
37 epidemiological purposes, health care treatment, insurance, payment,
38 or operations under the federal health insurance portability and
39 accountability act of 1996, or to X-ray, roentgen process, computed
40 tomography, magnetic resonance imaging, positron emission tomography

1 scan, mammography, or other image or film of the human anatomy used
2 exclusively to diagnose, prognose, or treat an illness or other
3 medical condition or to further validate scientific testing or
4 screening.

5 (4) To the extent the transaction requested by a consumer is a
6 controller's placement of that consumer's personal data in the public
7 domain, such as recording of a real estate deed showing name and
8 address, the controller has the same rights as any other person or
9 entity with regard to such information.

10 (5) This chapter does not apply to consumers sharing their
11 personal contact information such as email addresses with other
12 consumers in workplace, social, political or similar settings where
13 the purpose of the information is to facilitate communication among
14 such consumers, provided that any processing of such contact
15 information beyond interpersonal communication is covered by this
16 chapter. This chapter shall not apply to controllers' publication of
17 controller-based member or employee contact information where such
18 publication is intended to allow members of the public to contact
19 such member or employee in the ordinary course of the controller's
20 operations.

21 (6) Nothing in this chapter diminishes any consumer's or
22 controller's rights or obligations under chapter 70.02 RCW.

23 NEW SECTION. **Sec. 114.** LIMITATIONS AND APPLICABILITY. (1) The
24 obligations imposed on controllers or processors under this chapter
25 do not restrict a controller's or processor's ability to:

26 (a) Comply with federal, state, or local laws, rules, or
27 regulations;

28 (b) Comply with a civil, criminal, or regulatory inquiry,
29 investigation, subpoena, or summons by federal, state, local, or
30 other governmental authorities;

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

35 (d) Investigate, establish, exercise, prepare for, or defend
36 legal claims;

37 (e) Provide a product or service specifically requested by a
38 consumer, perform a contract to which the consumer is a party, or

1 take steps at the request of the consumer prior to entering into a
2 contract;

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

6 (g) Prevent, detect, protect against, or respond to security
7 incidents, identity theft, fraud, harassment, malicious or deceptive
8 activities, or any illegal activity; preserve the integrity or
9 security of systems; or investigate, report, or prosecute those
10 responsible for any such action;

11 (h) Engage in public or peer-reviewed scientific, historical, or
12 statistical research in the public interest that adheres to all other
13 applicable ethics and privacy laws and is approved, monitored, and
14 governed by an institutional review board, human subjects research
15 ethics review board, or a similar independent oversight entity that
16 determines: (i) If the research is likely to provide substantial
17 benefits that do not exclusively accrue to the controller; (ii) the
18 expected benefits of the research outweigh the privacy risks; and
19 (iii) if the controller has implemented reasonable safeguards to
20 mitigate privacy risks associated with research, including any risks
21 associated with reidentification; or

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

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

27 (a) Identify and repair technical errors that impair existing or
28 intended functionality; or

29 (b) Perform solely internal operations that are reasonably
30 aligned with the expectations of the consumer based on the consumer's
31 existing relationship with the controller, or are otherwise
32 compatible with processing in furtherance of the provision of a
33 product or service specifically requested by a consumer or the
34 performance of a contract to which the consumer is a party when those
35 internal operations are performed during, and not following, the
36 consumer's relationship with the controller.

37 (3) The obligations imposed on controllers or processors under
38 this chapter do not apply where compliance by the controller or
39 processor with this chapter would violate an evidentiary privilege
40 under Washington law and do not prevent a controller or processor

1 from providing personal data concerning a consumer to a person
2 covered by an evidentiary privilege under Washington law as part of a
3 privileged communication.

4 (4) A controller or processor that discloses personal data to a
5 third-party controller or processor in compliance with the
6 requirements of this chapter is not in violation of this chapter if
7 the recipient processes such personal data in violation of this
8 chapter, provided that, at the time of disclosing the personal data,
9 the disclosing controller or processor did not have actual knowledge
10 that the recipient intended to commit a violation. A third-party
11 controller or processor receiving personal data from a controller or
12 processor in compliance with the requirements of this chapter is
13 likewise not in violation of this chapter for the obligations of the
14 controller or processor from which it receives such personal data.

15 (5) Obligations imposed on controllers and processors under this
16 chapter shall not:

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

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

22 (6) Processing personal data solely for the purposes expressly
23 identified in subsection (1)(a) through (g) of this section does not,
24 by itself, make an entity a controller with respect to the
25 processing.

26 (7) If a controller processes personal data pursuant to an
27 exemption in this section, the controller bears the burden of
28 demonstrating that the processing qualifies for the exemption and
29 complies with the requirements in subsection (8) of this section.

30 (8)(a) Personal data that is processed by a controller pursuant
31 to this section must not be processed for any purpose other than
32 those expressly listed in this section.

33 (b) Personal data that is processed by a controller pursuant to
34 this section may be processed solely to the extent that such
35 processing is: (i) Necessary, reasonable, and proportionate to the
36 purposes listed in this section; (ii) adequate, relevant, and limited
37 to what is necessary in relation to the specific purpose or purposes
38 listed in this section; and (iii) insofar as possible, taking into
39 account the nature and purpose of processing the personal data,
40 subjected to reasonable administrative, technical, and physical

1 measures to protect the confidentiality, integrity, and accessibility
2 of the personal data, and to reduce reasonably foreseeable risks of
3 harm to consumers.

4 NEW SECTION. **Sec. 115.** PRIVATE RIGHT OF ACTION. (1) Any
5 consumer alleging a violation of this chapter or a regulation adopted
6 under this chapter may bring a civil action in any court of competent
7 jurisdiction. A consumer protected by this chapter may not be
8 required, as a condition of service or otherwise, to accept mandatory
9 arbitration of a claim under this chapter.

10 (2) A violation of this chapter or a regulation adopted under
11 this chapter with respect to the personal data of a consumer
12 constitutes a rebuttable presumption of harm to that consumer.

13 (3) In a civil action in which the plaintiff prevails, the court
14 may award:

15 (a) Liquidated damages of \$10,000 per violation or actual
16 damages, whichever is greater;

17 (b) Punitive damages; and

18 (c) Any other relief, including but not limited to an injunction,
19 that the court determines appropriate.

20 (4) In addition to any relief awarded pursuant to subsection (3)
21 of this section, the court shall award reasonable attorneys' fees and
22 costs to any prevailing plaintiff.

23 NEW SECTION. **Sec. 116.** ENFORCEMENT. (1) The attorney general
24 may bring an action in the name of the state, or as *parens patriae* on
25 behalf of persons residing in the state, to enforce this chapter. In
26 actions brought by the attorney general, the legislature finds: (a)
27 The practices covered by this chapter are matters vitally affecting
28 the public interest for the purpose of applying the consumer
29 protection act, chapter 19.86 RCW, and (b) a violation of this
30 chapter is not reasonable in relation to the development and
31 preservation of business, is an unfair or deceptive act in trade or
32 commerce, and an unfair method of competition for the purpose of
33 applying the consumer protection act, chapter 19.86 RCW.

34 (2) Until July 31, 2023, in the event of a controller's or
35 processor's violation under this chapter, prior to filing a
36 complaint, the attorney general must provide the controller or
37 processor with a warning letter identifying the specific provisions
38 of this chapter the attorney general alleges have been or are being

1 violated. If, after 30 days of issuance of the warning letter, the
2 attorney general believes the controller or processor has failed to
3 cure any alleged violation, the attorney general may bring an action
4 against the controller or processor as provided under this chapter.

5 (3) Beginning July 31, 2023, in determining a civil penalty under
6 this chapter, the court must consider, as mitigating factors, a
7 controller's or processor's good faith efforts to comply with the
8 requirements of this chapter and any actions to cure or remedy the
9 violations before an action is filed.

10 (4) All receipts from the imposition of civil penalties under
11 this chapter must be deposited into the consumer privacy account
12 created in section 117 of this act.

13 NEW SECTION. **Sec. 117.** CONSUMER PRIVACY ACCOUNT. The consumer
14 privacy account is created in the state treasury. All receipts from
15 the imposition of civil penalties under this chapter must be
16 deposited into the account. Moneys in the account may be spent only
17 after appropriation. Moneys in the account may only be used for the
18 purposes of recovery of costs and attorneys' fees accrued by the
19 attorney general in enforcing this chapter and for the office of
20 privacy and data protection as created in RCW 43.105.369. Moneys may
21 not be used to supplant general fund appropriations to either agency.

22 NEW SECTION. **Sec. 118.** If any provision of this act or its
23 application to any person or circumstance is held invalid, the
24 remainder of the act or the application of the provision to other
25 persons or circumstances is not affected.

26 NEW SECTION. **Sec. 119.** A new section is added to chapter 42.56
27 RCW to read as follows:

28 Data protection assessments submitted by a controller to the
29 attorney general in accordance with requirements under section 112 of
30 this act are exempt from disclosure under this chapter.

31 NEW SECTION. **Sec. 120.** A new section is added to chapter 44.28
32 RCW to read as follows:

33 (1) By December 1, 2023, the joint committee must review the
34 efficacy of the attorney general providing controllers and processors
35 with warning letters and 30 days to cure alleged violations in the
36 warning letters pursuant to section 116 of this act and report its

1 findings to the governor and the appropriate committees of the
2 legislature.

3 (2) The report must include, but not be limited to:

4 (a) The number of warning letters the attorney general sent to
5 controllers and processors;

6 (b) A list of the controller and processor names that received
7 the warning letters;

8 (c) The categories of violations and the number of violations per
9 category;

10 (d) The number of actions brought by the attorney general as
11 authorized in this act due to a controller or processor not curing
12 the alleged violations within 30 days;

13 (e) The types of resources, including associated costs, expended
14 when providing warning letters and tracking compliance; and

15 (f) A recommendation on whether the warning letters provided by
16 the attorney general should be continued.

17 (3) The office of the attorney general shall provide the joint
18 committee any data within their purview that the joint committee
19 considers necessary to conduct the review.

20 (4) This section expires June 30, 2024.

21 NEW SECTION. **Sec. 121.** Sections 101 through 117 of this act
22 constitute a new chapter in Title 19 RCW.

23 NEW SECTION. **Sec. 122.** Sections 1, 2, and 101 through 120 of
24 this act take effect July 31, 2022.

25 NEW SECTION. **Sec. 123.** Sections 101 through 117 of this act do
26 not apply to institutions of higher education or nonprofit
27 corporations until July 31, 2026."

28 Correct the title.

EFFECT: Strikes Part 2 and Part 3 of the bill relating to the
processing of data collected by private and public entities for
certain public health emergency and contact tracing purposes. Removes
provisions related to the stricken parts of the bill from the
legislative intent section.

Makes the following changes in Part 1 of the bill relating to
consumer personal data privacy:

Key Definitions and Jurisdictional Scope:

(1) Adds the definitions of "biometric information," "device,"
"harm," "monetize," and "Washington governmental entity."

(2) Modifies the definition of "personal data."

(3) Specifies that exchanging personal data for monetary or other valuable consideration or otherwise profiting constitutes "sale" regardless of whether the consumer's personal data changes hands.

(4) Applies the requirements of the bill to legal entities that, during a calendar year, process the personal data of at least 1,000 consumers, rather than 100,000 consumers, or that earn \$10,000,000 in annual revenue through at least 300 transactions, rather than derive 25 percent of gross revenue from the sale of data.

(5) Provides that state agencies, legislative agencies, the judicial branch, local governments, tribes, and municipal corporations are not exempt from the provisions related to biometric information.

Opt-in Consent:

(6) Requires controllers to obtain a consumer's opt-in consent before processing the consumer's personal data or making any changes in the processing that would necessitate a change to the required privacy notice.

(7) Requires the opt-in consent to be renewed not less than annually and the option to withhold consent to be presented as clearly and prominently as the option to provide consent.

(8) Requires controllers to provide a mechanism to withdraw consent at any time.

Consumer Rights:

(9) Strikes from the right to correct inaccurate personal data the requirement to take into consideration the nature of the personal data and the purposes of processing.

(10) Removes the right to opt out of the processing for certain purposes and instead provides that a consumer has the right to refuse consent for any processing of the consumer's personal data.

(11) Strikes provisions related to opting out of processing via global privacy controls or by designating an authorized agent.

(12) Provides that a consumer has the right to not be subject to surreptitious surveillance and prohibits controllers from activating a microphone, camera, or any other sensor capable of collecting or transmitting personal data without first providing the required privacy notice and obtaining opt-in consent, which is to expire after 90 days unless renewed by the consumer.

Biometric Information:

(13) Defines the obligations of controllers and Washington governmental entities relating to biometric information, including: Informing consumers that biometric information is being processed; obtaining opt-in consent; establishing retention schedules and guidelines for permanently destroying biometric information; disclosing biometric information only if specified circumstances exist; and prohibiting monetization of biometric information unless limited exceptions apply.

Exceptions to the Consent Requirement:

(14) Specifies the circumstances when controllers and Washington governmental entities are not required to obtain opt-in consent for processing of personal data or biometric information, including: Processing is necessary to execute the specific transaction requested by a consumer; in cases of emergency, if specified requirements are met; disclosure is required by state or federal law or to respond to a warrant or subpoena, if specified requirements are met; or processing involves only deidentified information.

(15) Exempts certain health-related personal data and biometric information, as well as the sharing of personal contact information by consumers for purposes of interpersonal communication.

Enforcement:

(16) Modifies the provisions related to a private right of and provides that a consumer alleging a violation may bring a civil action and recover liquidated damages of \$10,000 per violation or actual damages, whichever is greater, punitive damages, and any other relief that the court determines appropriate.

Preemption:

(17) Removes the provisions that preempt local laws and regulations regarding the processing of personal data.

Studies and Reports:

(18) Directs the Department of Commerce to conduct a study to determine the most effective way for controllers to obtain consumers' consent and adopt regulation related to opt-in consent.

(19) Requires the Joint Legislative Audit and Review Committee study on the efficacy of the Attorney General providing warning letters to controllers and processors to be completed by December 1, 2023, rather than December 1, 2025.

(20) Strikes the provisions requiring the Office of Privacy and Data Protection to complete a study and submit a report on the development of technology related to opting out of the processing of personal data.

--- END ---