

---

**SENATE BILL 5376**

---

**State of Washington**

**66th Legislature**

**2019 Regular Session**

**By** Senators Carlyle, Palumbo, Wellman, Mullet, Pedersen, Billig, Hunt, Lias, Rolfes, Saldaña, Hasegawa, and Keiser

Read first time 01/18/19. Referred to Committee on Environment, Energy & Technology.

1 AN ACT Relating to the management and oversight of personal data;  
2 amending RCW 43.105.369; adding a new section to chapter 9.73 RCW;  
3 adding a new chapter to Title 19 RCW; creating new sections;  
4 prescribing penalties; and providing an effective date.

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

6 NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and  
7 cited as the Washington privacy act.

8 NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS. (1) The legislature  
9 finds that:

10 (a) Washingtonians cherish privacy as an element of their  
11 individual freedom.

12 (b) Washington is a technology leader on a national and global  
13 level and recognizes its distinctive position in promoting the  
14 efficient balance of consumer privacy and economic benefits.

15 (c) Washington explicitly recognizes its citizens' right to  
16 privacy under Article I, section 7 of the state Constitution.

17 (d) There is rapid growth in the volume and variety of personal  
18 data being generated, collected, stored, and analyzed. This growth  
19 has the potential for great benefits to human knowledge,

1 technological innovation, and economic growth, but also the potential  
2 to harm individual privacy and freedom.

3 (e) Millions of Washingtonians have been affected by electronic  
4 data breaches and the resulting loss of privacy, and the net effect,  
5 both financially and in the chilling of consumer confidence, has and  
6 will continue to cost Washington state businesses.

7 (f) As technology and businesses continue to push the limits of  
8 data collection with exponential rapidity, laws must keep pace as  
9 technology and business practices evolve to protect businesses and  
10 consumers.

11 (g) There is a need to preserve individuals' trust and confidence  
12 that personal data will be protected appropriately, while supporting  
13 flexibility and the free flow of information. Meeting this need will  
14 promote continued innovation and economic growth in the networked  
15 economy.

16 (h) Enforcement of general principles in law will ensure that  
17 citizens continue to enjoy meaningful privacy protections while  
18 affording ample flexibility for technologies and business models to  
19 evolve.

20 (i) The European Union recently updated its privacy law through  
21 the passage and implementation of the general data protection  
22 regulation, affording its residents the strongest privacy protections  
23 in the world. Washington residents deserve to enjoy the same level of  
24 robust privacy safeguards.

25 (j) In addition, the technology industry has been a tremendous  
26 driver of economic growth in Washington state. We need to ensure that  
27 any new privacy laws not only provide Washington residents with  
28 strong privacy protections but also enable industry and others to use  
29 data to create innovative technologies, products, and solutions.

30 (k) Technology will continue to evolve and change. Consequently,  
31 any new privacy laws must be technology neutral and flexible, so that  
32 they may apply not only to the technologies and products of today,  
33 but to the technologies and products of tomorrow.

34 (l) Washington residents have long enjoyed an expectation of  
35 privacy in their public movements. The development of new technology  
36 like facial recognition could, if deployed indiscriminately and  
37 without guardrails, enable the constant surveillance of any  
38 individual any time of the day and every day of the year. Washington  
39 residents should have the right to a reasonable expectation of  
40 privacy in their movements, and thus should be free from ubiquitous

1 and surreptitious surveillance using facial recognition technology.  
2 Further, Washington residents should have the right to expect  
3 information about the capabilities and limitations of facial  
4 recognition technology and that it should not be deployed by private  
5 sector organizations without proper public notice.

6 (2) As such, the legislature recognizes the consumer protection  
7 principles in this act regarding transparency, individual control,  
8 respect for context, focused collection and responsible use,  
9 security, access, and accuracy.

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

13 (1) "Affiliate" means a legal entity that controls, is controlled  
14 by, or is under common control with, another legal entity.

15 (2) "Consent" means a clear affirmative act establishing a freely  
16 given, specific, informed, and unambiguous indication of a consumer's  
17 agreement to the processing of personal data relating to the  
18 consumer, such as by a written statement or other clear affirmative  
19 action.

20 (3) "Consumer" means a natural person who is a Washington  
21 resident. It does not include an employee or contractor of a business  
22 acting in their role as an employee or contractor.

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

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

30 (6) "Deidentified data" means:

31 (a) Data that cannot be linked to a known natural person without  
32 additional information kept separately; or

33 (b) Data (i) that has been modified to a degree that the risk of  
34 reidentification is small, (ii) that is subject to a public  
35 commitment by the controller not to attempt to reidentify the data,  
36 and (iii) to which one or more enforceable controls to prevent  
37 reidentification has been applied. Enforceable controls to prevent  
38 reidentification may include legal, administrative, technical, or  
39 contractual controls.

1 (7) "Developer" means a person who creates or modifies the set of  
2 instructions or programs instructing a computer or device to perform  
3 tasks.

4 (8) "Identified or identifiable natural person" means a person  
5 who can be identified, directly or indirectly, in particular by  
6 reference to an identifier such as a name, an identification number,  
7 specific geolocation data, or an online identifier.

8 (9) "Minor" means any person under eighteen years of age.

9 (10) "Personal data" means any information relating to an  
10 identified or identifiable natural person. Personal data does not  
11 include deidentified data.

12 (11) "Process" or "processing" means any operation or set of  
13 operations that is performed on personal data or on sets of personal  
14 data, whether or not by automated means, such as collection,  
15 recording, organization, structuring, storage, adaptation or  
16 alteration, retrieval, consultation, use, disclosure by transmission,  
17 dissemination or otherwise making available, alignment or  
18 combination, restriction, deletion, or destruction.

19 (12) "Processor" means a natural or legal person which processes  
20 personal data on behalf of the controller.

21 (13) "Profiling" means any form of automated processing of  
22 personal data consisting of the use of personal data to evaluate  
23 certain personal aspects relating to a natural person, in particular  
24 to analyze or predict aspects concerning that natural person's  
25 economic situation, health, personal preferences, interests,  
26 reliability, behavior, location, or movements.

27 (14) "Restriction of processing" means the marking of stored  
28 personal data with the aim of limiting the processing of such  
29 personal data in the future.

30 (15)(a) "Sale" means the exchange of personal data for monetary  
31 consideration by the controller to a third party for purposes of  
32 licensing or selling personal data at the third party's discretion to  
33 additional third parties.

34 (b) "Sale" does not include the following: (i) The disclosure of  
35 personal data to a processor who processes the personal data on  
36 behalf of the controller; or (ii) the disclosure of personal data to  
37 a third party with whom the consumer has a direct relationship for  
38 purposes of providing a product or service requested by the consumer  
39 or otherwise in a manner that is consistent with a consumer's

1 reasonable expectations considering the context in which the consumer  
2 provided the personal data to the controller.

3 (16) "Sensitive data" means personal data revealing racial or  
4 ethnic origin, religious or philosophical beliefs, and the processing  
5 of genetic data, biometric data for the purpose of uniquely  
6 identifying a natural person, data concerning a minor, data  
7 concerning health, or data concerning a natural person's sex life or  
8 sexual orientation.

9 (17) "Targeted advertising" means displaying advertisements to a  
10 consumer where the advertisement is selected based on personal data  
11 obtained or inferred over time from a consumer's activities across  
12 nonaffiliate web sites, applications, or online services. It does not  
13 include advertising to a consumer based upon the consumer's current  
14 visit to a web site, application, or online service, or in response  
15 to the consumer's request for information or feedback.

16 NEW SECTION. **Sec. 4.** JURISDICTIONAL SCOPE. (1) This chapter  
17 applies to legal entities that conduct business in Washington or  
18 produce products or services that are intentionally targeted to  
19 residents of Washington, and that satisfy one or more of the  
20 following thresholds:

21 (a) Controls or processes data of one hundred thousand consumers  
22 or more; or

23 (b) Derives over fifty percent of gross revenue from the sale of  
24 personal information and processes or controls personal information  
25 of twenty-five thousand consumers or more.

26 (2) This chapter does not apply to:

27 (a) State and local governments;

28 (b) Personal data sets to the extent that they are regulated by  
29 the federal health insurance portability and accountability act of  
30 1996, the federal health information technology for economic and  
31 clinical health act, or the Gramm-Leach-Bliley act of 1999; or

32 (c) Data sets maintained for employment records purposes.

33 NEW SECTION. **Sec. 5.** RESPONSIBILITY ACCORDING TO ROLE. (1)  
34 Controllers shall be responsible for meeting the obligations set  
35 forth under this act.

36 (2) Processors are responsible under this act for adhering to the  
37 instructions of the controller and assisting the controller to meet  
38 its obligations under this chapter.

1 (3) Processing by a processor shall be governed by a contract  
2 between the controller and the processor that is binding on the  
3 processor and that sets out the processing instructions to which the  
4 processor is bound.

5 NEW SECTION. **Sec. 6.** CONSUMER RIGHTS. Controllers shall  
6 facilitate requests to exercise the consumer rights set forth in  
7 subsections (1) through (7) of this section.

8 (1) On request from a consumer, a controller must confirm whether  
9 or not personal data concerning the consumer is being processed by  
10 the controller, including whether such personal data is sold to data  
11 brokers, and, where personal data concerning the consumer is being  
12 processed by the controller, provide access to such personal data  
13 concerning the consumer.

14 (a) On request from a consumer, a controller must provide a copy  
15 of the personal data undergoing processing. For any further copies  
16 requested by the consumer, the controller may charge a reasonable fee  
17 based on administrative costs. Where the consumer makes the request  
18 by electronic means, and unless otherwise requested by the consumer,  
19 the information must be provided in a commonly used electronic form.

20 (b) This subsection shall not adversely affect the rights of  
21 consumers.

22 (2) On request from a consumer, the controller, without undue  
23 delay, must correct inaccurate personal data concerning the consumer.  
24 Taking into account the purposes of the processing, the controller  
25 must complete incomplete personal data, including by means of  
26 providing a supplementary statement.

27 (3)(a) On request from a consumer, a controller must delete the  
28 consumer's personal data without undue delay where one of the  
29 following grounds applies:

30 (i) The personal data is no longer necessary in relation to the  
31 purposes for which the personal data was collected or otherwise  
32 processed;

33 (ii) For processing that requires consent under section 8(3) of  
34 this act, the consumer withdraws consent to processing and there are  
35 no other legitimate grounds for the processing;

36 (iii) The consumer objects to the processing pursuant to  
37 subsection (6) of this section and (A) there are no overriding  
38 legitimate grounds for the processing; or (B) the processing is for  
39 direct marketing purposes;

1 (iv) The personal data has been unlawfully processed;

2 (v) The personal data must be deleted to comply with a legal  
3 obligation under federal, state, or local law to which the controller  
4 is subject; or

5 (vi) The personal data has been collected in relation to the  
6 offer of a service normally provided for remuneration, at a distance,  
7 by electronic means, and at the individual request of the recipient  
8 of services.

9 (b) Where the controller is obliged to delete personal data under  
10 this section that has been disclosed to third parties by the  
11 controller, including data brokers that received the data through a  
12 sale, the controller must take reasonable steps, which may include  
13 technical measures, to inform other controllers that are processing  
14 the personal data that the consumer has requested the deletion by the  
15 other controllers of any links to, or copy or replication of, the  
16 personal data. Compliance with this obligation must take into account  
17 available technology and cost of implementation.

18 (c) This subsection does not apply to the extent processing is  
19 necessary:

20 (i) For exercising the right of free speech;

21 (ii) For compliance with a legal obligation that requires  
22 processing by federal, state, or local law to which the controller is  
23 subject or for the performance of a task carried out in the public  
24 interest or in the exercise of official authority vested in the  
25 controller;

26 (iii) For reasons of public interest in the area of public  
27 health, where the processing (A) is subject to suitable and specific  
28 measures to safeguard the rights of the consumer; and (B) is  
29 processed by or under the responsibility of a professional subject to  
30 confidentiality obligations under federal, state, or local law;

31 (iv) For archiving purposes in the public interest, scientific or  
32 historical research purposes, or statistical purposes, where the  
33 deletion of such personal data is likely to render impossible or  
34 seriously impair the achievement of the objectives of the processing;  
35 or

36 (v) For the establishment, exercise, or defense of legal claims.

37 (4)(a) On request from a consumer, the controller must restrict  
38 processing if one of the following grounds applies:

1 (i) The accuracy of the personal data is contested by the  
2 consumer, for a period enabling the controller to verify the accuracy  
3 of the personal data;

4 (ii) The processing is unlawful and the consumer opposes the  
5 deletion of the personal data and requests the restriction of  
6 processing instead;

7 (iii) The controller no longer needs the personal data for the  
8 purposes of the processing, but such personal data is required by the  
9 consumer for the establishment, exercise, or defense of legal claims;  
10 or

11 (iv) The consumer objects to the processing pursuant to  
12 subsection (6) of this section pending the verification of whether  
13 the legitimate grounds of the controller override those of the  
14 consumer.

15 (b) Where personal data is subject to a restriction of processing  
16 under this subsection, the personal data must, with the exception of  
17 storage, only be processed (i) with the consumer's consent; (ii) for  
18 the establishment, exercise, or defense of legal claims; (iii) for  
19 the protection of the rights of another natural or legal person; or  
20 (iv) for reasons of important public interest under federal, state,  
21 or local law.

22 (c) A consumer who has obtained restriction of processing  
23 pursuant to this subsection must be informed by the controller before  
24 the restriction of processing is lifted.

25 (5)(a) On request from a consumer, the controller must provide  
26 the consumer any personal data concerning such consumer that such  
27 consumer has provided to the controller in a structured, commonly  
28 used, and machine-readable format if (i)(A) the processing of such  
29 personal data requires consent under section 8(3) of this act, (B)  
30 the processing of such personal data is necessary for the performance  
31 of a contract to which the consumer is a party, or (C) in order to  
32 take steps at the request of the consumer prior to entering into a  
33 contract; and (ii) the processing is carried out by automated means.

34 (b) Controllers must transmit the personal data requested under  
35 this subsection directly from one controller to another, where  
36 technically feasible, and transmit the personal data to another  
37 controller without hindrance from the controller to which the  
38 personal data was provided.

39 (c) Requests for personnel data under this subsection must be  
40 without prejudice to subsection (3) of this section.



1 (d) The rights provided in this subsection do not apply to  
2 processing necessary for the performance of a task carried out in the  
3 public interest or in the exercise of official authority vested in  
4 the controller, and must not adversely affect the rights of others.

5 (6)(a) A consumer may object, on grounds relating to the  
6 consumer's particular situation, at any time to processing of  
7 personal data concerning such consumer:

8 (b) When a consumer objects to direct marketing, which includes  
9 the sale of personal data concerning the consumer to third parties  
10 for direct marketing purposes, profiling to the extent that it is  
11 related to such direct marketing and targeted advertising, the  
12 controller must no longer process the personal data subject to the  
13 objection for such purpose and must communicate the consumer's  
14 objection, unless it proves impossible or involves disproportionate  
15 effort, regarding any further processing of the consumer's personal  
16 data for such purposes to any third parties to whom the controller  
17 sold the consumer's personal data for such purposes. Third parties  
18 must honor objection requests pursuant to this subsection received  
19 from third-party controllers.

20 (c) If a consumer objects to processing for any purposes, other  
21 than direct marketing, the controller may continue processing the  
22 personal data subject to the objection if the controller can  
23 demonstrate a compelling legitimate ground to process such personal  
24 data.

25 (7) A consumer must not be subject to a decision based solely on  
26 profiling which produces legal effects concerning such consumer or  
27 similarly significantly affects the consumer. Legal or similarly  
28 significant effects include, but are be limited to, denial of  
29 consequential services or support, such as financial and lending  
30 services, housing, insurance, education enrollment, criminal justice,  
31 employment opportunities, and health care services.

32 (a) This subsection does not apply if the decision is:

33 (i) Necessary for entering into, or performance of, a contract  
34 between the consumer and a controller;

35 (ii) Authorized by federal or state law to which the controller  
36 is subject and which incorporates suitable measures to safeguard the  
37 consumer's rights and legitimate interests, as indicated by the risk  
38 assessments required by section 8 of this act; or

39 (iii) Based on the consumer's consent.

1 (b) Notwithstanding (a) of this subsection, the controller shall  
2 implement suitable measures to safeguard consumer's rights and  
3 legitimate interests with respect to decisions based solely on  
4 profiling, including providing human review of the decision, to  
5 express the consumer's point of view with respect to the decision,  
6 and to contest the decision.

7 (8) A controller must communicate any correction, deletion, or  
8 restriction of processing carried out in accordance with subsections  
9 (2), (3), or (4) of this section to each third-party recipient to  
10 whom the personal data has been disclosed, including third parties  
11 that received the data through a sale, unless this proves impossible  
12 or involves disproportionate effort. The controller must inform the  
13 consumer about such third-party recipients, if any, if the consumer  
14 requests such information.

15 (9) A controller must provide information on action taken on a  
16 request under subsections (1) through (7) of this section without  
17 undue delay and in any event within thirty days of receipt of the  
18 request. That period may be extended by sixty additional days where  
19 necessary, taking into account the complexity and number of the  
20 requests. The controller must inform the consumer of any such  
21 extension within thirty days of receipt of the request, together with  
22 the reasons for the delay. Where the consumer makes the request by  
23 electronic means, the information must be provided by electronic  
24 means where possible, unless otherwise requested by the consumer.

25 (a) If a controller does not take action on the request of a  
26 consumer, the controller must inform the consumer without undue delay  
27 and at the latest within thirty days of receipt of the request of the  
28 reasons for not taking action and any possibility for internal review  
29 of the decision by the controller.

30 (b) Information provided under this section must be provided by  
31 the controller free of charge to the consumer. Where requests from a  
32 consumer are manifestly unfounded or excessive, in particular because  
33 of their repetitive character, the controller may either: (i) Charge  
34 a reasonable fee taking into account the administrative costs of  
35 providing the information or communication or taking the action  
36 requested; or (ii) refuse to act on the request. The controller bears  
37 the burden of demonstrating the manifestly unfounded or excessive  
38 character of the request.

39 (c) Where the controller has reasonable doubts concerning the  
40 identity of the consumer making a request under subsections (1)

1 through (7) of this section, the controller may request the provision  
2 of additional information necessary to confirm the identity of the  
3 consumer.

4 NEW SECTION. **Sec. 7.** TRANSPARENCY. (1) Controllers must be  
5 transparent and accountable for their processing of personal data, by  
6 making available in a form that is reasonably accessible to consumers  
7 a clear, meaningful privacy notice that includes:

- 8 (a) The categories of personal data collected by the controller;
- 9 (b) The purposes for which the categories of personal data is  
10 used and disclosed to third parties, if any;
- 11 (c) The rights that consumers may exercise pursuant to section 6  
12 of this act, if any;
- 13 (d) The categories of personal data that the controller shares  
14 with third parties, if any; and
- 15 (e) The categories of third parties, if any, with whom the  
16 controller shares personal data.

17 (2) Controllers that engage in profiling must disclose such  
18 profiling to the consumer at or before the time personal data is  
19 obtained, including meaningful information about the logic involved  
20 and the significance and envisaged consequences of the profiling.

21 (3) If a controller sells personal data to data brokers or  
22 processes personal data for direct marketing purposes, including  
23 targeted marketing and profiling to the extent that it is related to  
24 such direct marketing, it must disclose such processing, as well as  
25 the manner in which a consumer may exercise the right to object to  
26 such processing, in a clear and prominent manner.

27 NEW SECTION. **Sec. 8.** DOCUMENTED RISK ASSESSMENTS. (1)  
28 Controllers must conduct and document risk assessments covering the  
29 processing of personal data prior to the processing of such personal  
30 data whenever there is a change in processing that materially impacts  
31 the risk to individuals, and on at least an annual basis regardless  
32 of changes in processing. Risk assessments must take into account the  
33 type of personal data to be processed by the controller, including  
34 the extent to which the personal data is sensitive data or otherwise  
35 sensitive in nature, and the context in which the personal data is to  
36 be processed.

37 (2) Risk assessments conducted under subsection (1) of this  
38 section must identify and weigh the benefits that may flow directly

1 and indirectly from the processing to the controller, consumer, other  
2 stakeholders, and the public, against the potential risks to the  
3 rights of the consumer associated with such processing, as mitigated  
4 by safeguards that can be employed by the controller to reduce such  
5 risks. The use of deidentified data and the reasonable expectations  
6 of consumers must factor into this assessment by the controller.

7 (3) If the risk assessment conducted under subsection (1) of this  
8 section determines that the potential risks to the rights of the  
9 consumer outweigh the interests of the controller, consumer, other  
10 stakeholders, and the public in processing the personal data of the  
11 consumer, the controller may only engage in such processing with the  
12 consent of the consumer. Such consent shall be as easy to withdraw as  
13 to give.

14 (4) The controller must make the risk assessment available to the  
15 attorney general upon request. Risk assessments are confidential and  
16 exempt from public inspection and copying under chapter 42.56 RCW.

17 NEW SECTION. **Sec. 9.** DEIDENTIFIED DATA. A controller or  
18 processor that uses deidentified data must exercise reasonable  
19 oversight to monitor compliance with any contractual commitments to  
20 which the deidentified data is subject, and must take appropriate  
21 steps to address any breaches of contractual commitments.

22 NEW SECTION. **Sec. 10.** EXEMPTIONS. (1) The obligations imposed  
23 on controllers or processors under this chapter do not restrict a  
24 controller's or processor's ability to:

- 25 (a) Comply with federal, state, or local laws;
- 26 (b) Comply with a civil, criminal, or regulatory inquiry,  
27 investigation, subpoena, or summons by federal, state, local, or  
28 other governmental authorities;
- 29 (c) Cooperate with law enforcement agencies concerning conduct or  
30 activity that the controller or processor reasonably and in good  
31 faith believes may violate federal, state, or local law;
- 32 (d) Investigate, exercise, or defend legal claims; or
- 33 (e) Prevent or detect identity theft, fraud, or other criminal  
34 activity or verify identities.

35 (2) The obligations imposed on controllers or processors under  
36 this chapter do not apply where compliance by the controller or  
37 processor with this chapter would violate an evidentiary privilege  
38 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 (3) 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,  
7 including under section 11 of this act, if the third-party recipient  
8 processes such personal data in violation of this chapter, provided  
9 that, at the time of disclosing the personal data, the disclosing  
10 controller or processor did not have actual knowledge that the third-  
11 party recipient intended to commit a violation. A third-party  
12 recipient receiving personal data from a controller or processor is  
13 likewise not liable under this chapter, including under section 11 of  
14 this act, for the obligations of a controller or processor to which  
15 it provides services.

16 (4) This chapter does not require a controller or processor to do  
17 the following:

18 (a) Reidentify deidentified data;

19 (b) Retain personal data concerning a consumer that it would not  
20 otherwise retain in the ordinary course of business;

21 (c) Comply with a request to exercise any of the rights under  
22 section 6 (1) through (7) of this act if the controller is unable to  
23 verify, using commercially reasonable efforts, the identity of the  
24 consumer making the request.

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

27 (a) Adversely affect the rights of any persons; or

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

30 NEW SECTION. **Sec. 11.** LIABILITY. (1) This chapter does not  
31 serve as the basis for a private right of action under this chapter  
32 or any other law.

33 (2) Where more than one controller or processor, or both a  
34 controller and a processor, involved in the same processing, is in  
35 violation of this chapter, the liability shall be allocated among the  
36 parties according to principles of comparative fault, unless such  
37 liability is otherwise allocated by contract among the parties.

1        NEW SECTION.    **Sec. 12.**    ENFORCEMENT. (1) The legislature finds  
2 that the practices covered by this chapter are matters vitally  
3 affecting the public interest for the purpose of applying the  
4 consumer protection act, chapter 19.86 RCW. A violation of this  
5 chapter is not reasonable in relation to the development and  
6 preservation of business and is an unfair or deceptive act in trade  
7 or commerce and an unfair method of competition for the purpose of  
8 applying the consumer protection act, chapter 19.86 RCW.

9        (2) The attorney general may bring an action in the name of the  
10 state, or as parens patriae on behalf of persons residing in the  
11 state, to enforce this chapter.

12        (3) A controller or processor is in violation of this chapter if  
13 it fails to cure any alleged breach of sections 7 through 10 of this  
14 act within thirty days after receiving notice of alleged  
15 noncompliance. Any controller or processor that violates this chapter  
16 is subject to an injunction and liable for a civil penalty of not  
17 more than two thousand five hundred dollars for each violation or  
18 seven thousand five hundred dollars for each intentional violation.

19        (4) The consumer privacy account is created in the state  
20 treasury. All receipts from the imposition of civil penalties under  
21 this chapter must be deposited into the account. Moneys in the  
22 account may be spent only after appropriation. Expenditures from the  
23 account may be used only to fund the office of privacy and data  
24 protection as established under RCW 43.105.369.

25        NEW SECTION.    **Sec. 13.**    PREEMPTION. This chapter supersedes and  
26 preempts laws adopted by any local entity regarding the processing of  
27 personal data by controllers or processors.

28        NEW SECTION.    **Sec. 14.**    FACIAL RECOGNITION. (1) Controllers using  
29 facial recognition for profiling must employ meaningful human review  
30 prior to making final decisions based on such profiling where such  
31 final decisions produce legal effects concerning consumers or  
32 similarly significant effects concerning consumers. Decisions  
33 producing legal effects or similarly significant effects shall  
34 include, but not be limited to, denial of consequential services or  
35 support, such as financial and lending services, housing, insurance,  
36 education enrollment, criminal justice, employment opportunities, and  
37 health care services.

1 (2) Processors that provide facial recognition services must  
2 provide documentation that includes general information that explains  
3 the capabilities and limitations of the technology in terms that  
4 customers and consumers can understand.

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 such 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 obtain consent from consumers prior to  
11 deploying facial recognition services. The placement of conspicuous  
12 notice in physical premises or online that clearly conveys that  
13 facial recognition services are being used constitute a consumer's  
14 consent to the use of such facial recognition services when that  
15 consumer enters those premises or proceeds to use the online services  
16 that have such notice, provided that there is a means by which the  
17 consumer may exercise choice as to facial recognition services.

18 (5) Providers of commercial facial recognition services that make  
19 their technology available as an online service for developers and  
20 customers to use in their own scenarios must make available an  
21 application programming interface or other technical capability,  
22 chosen by the provider, to enable third parties that are legitimately  
23 engaged in independent testing to conduct reasonable tests of those  
24 facial recognition services for accuracy and unfair bias.

25 (6) For purposes of this section, "facial recognition" means  
26 technology that analyzes facial features and is used for the unique  
27 personal identification of natural persons in still or video images.

28 NEW SECTION. **Sec. 15.** A new section is added to chapter 9.73  
29 RCW to read as follows:

30 (1) State and local government agencies shall not use facial  
31 recognition technology to engage in ongoing surveillance of specified  
32 individuals in public spaces, unless such use is in support of law  
33 enforcement activities and either (a) a court order has been obtained  
34 to permit the use of facial recognition services for that ongoing  
35 surveillance; or (b) where there is an emergency involving imminent  
36 danger or risk of death or serious physical injury to a person.

37 (2) This section applies to all Washington state and local  
38 government agencies.

1 (3) For purposes of this section, "facial recognition" means the  
2 same as in section 14 of this act.

3 **Sec. 16.** RCW 43.105.369 and 2016 c 195 s 2 are each amended to  
4 read as follows:

5 (1) The office of privacy and data protection is created within  
6 the office of the state chief information officer. The purpose of the  
7 office of privacy and data protection is to serve as a central point  
8 of contact for state agencies on policy matters involving data  
9 privacy and data protection.

10 (2) The director shall appoint the chief privacy officer, who is  
11 the director of the office of privacy and data protection.

12 (3) The primary duties of the office of privacy and data  
13 protection with respect to state agencies are:

14 (a) To conduct an annual privacy review;

15 (b) To conduct an annual privacy training for state agencies and  
16 employees;

17 (c) To articulate privacy principles and best practices;

18 (d) To coordinate data protection in cooperation with the agency;  
19 and

20 (e) To participate with the office of the state chief information  
21 officer in the review of major state agency projects involving  
22 personally identifiable information.

23 (4) The office of privacy and data protection must serve as a  
24 resource to local governments and the public on data privacy and  
25 protection concerns by:

26 (a) Developing and promoting the dissemination of best practices  
27 for the collection and storage of personally identifiable  
28 information, including establishing and conducting a training program  
29 or programs for local governments; and

30 (b) Educating consumers about the use of personally identifiable  
31 information on mobile and digital networks and measures that can help  
32 protect this information.

33 (5) By December 1, 2016, and every four years thereafter, the  
34 office of privacy and data protection must prepare and submit to the  
35 legislature a report evaluating its performance. The office of  
36 privacy and data protection must establish performance measures in  
37 its 2016 report to the legislature and, in each report thereafter,  
38 demonstrate the extent to which performance results have been



1 achieved. These performance measures must include, but are not  
2 limited to, the following:

3 (a) The number of state agencies and employees who have  
4 participated in the annual privacy training;

5 (b) A report on the extent of the office of privacy and data  
6 protection's coordination with international and national experts in  
7 the fields of data privacy, data protection, and access equity;

8 (c) A report on the implementation of data protection measures by  
9 state agencies attributable in whole or in part to the office of  
10 privacy and data protection's coordination of efforts; and

11 (d) A report on consumer education efforts, including but not  
12 limited to the number of consumers educated through public outreach  
13 efforts, as indicated by how frequently educational documents were  
14 accessed, the office of privacy and data protection's participation  
15 in outreach events, and inquiries received back from consumers via  
16 telephone or other media.

17 (6) Within one year of June 9, 2016, the office of privacy and  
18 data protection must submit to the joint legislative audit and review  
19 committee for review and comment the performance measures developed  
20 under subsection (5) of this section and a data collection plan.

21 (7) The office of privacy and data protection shall submit a  
22 report to the legislature on the: (a) Extent to which  
23 telecommunications providers in the state are deploying advanced  
24 telecommunications capability; and (b) existence of any inequality in  
25 access to advanced telecommunications infrastructure experienced by  
26 residents of tribal lands, rural areas, and economically distressed  
27 communities. The report may be submitted at a time within the  
28 discretion of the office of privacy and data protection, at least  
29 once every four years, and only to the extent the office of privacy  
30 and data protection is able to gather and present the information  
31 within existing resources.

32 (8) The office of privacy and data protection must conduct an  
33 analysis on the public sector use of facial recognition. By September  
34 30, 2023, the office of privacy and data protection must submit a  
35 report of its findings to the appropriate committees of the  
36 legislature.

37 NEW SECTION. **Sec. 17.** Sections 3 through 14 of this act  
38 constitute a new chapter in Title 19 RCW.

1        NEW SECTION.    **Sec. 18.**    This act takes effect December 31, 2020.

--- **END** ---