

---

**SUBSTITUTE SENATE BILL 6280**

---

**State of Washington**

**66th Legislature**

**2020 Regular Session**

**By** Senate Environment, Energy & Technology (originally sponsored by Senators Nguyen, Carlyle, Wellman, Salomon, Lovelett, Das, Randall, Pedersen, Wilson, C., and Hunt)

1 AN ACT Relating to the use of facial recognition services; adding  
2 a new section to chapter 9.73 RCW; adding a new chapter to Title 43  
3 RCW; creating a new section; and providing an expiration date.

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

5 NEW SECTION. **Sec. 1.** The legislature finds that:

6 (1) Unconstrained use of facial recognition services by state and  
7 local government agencies poses broad social ramifications that  
8 should be considered and addressed. Accordingly, legislation is  
9 required to establish safeguards that will allow state and local  
10 government agencies to use facial recognition services in a manner  
11 that benefits society while prohibiting uses that threaten our  
12 democratic freedoms and put our civil liberties at risk.

13 (2) However, state and local government agencies may use facial  
14 recognition services in a variety of beneficial ways, such as  
15 locating missing or incapacitated persons, identifying victims of  
16 crime, and keeping the public safe.

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

1 (1) "Accountability report" means a report developed in  
2 accordance with section 3 of this act.

3 (2) "Enroll," "enrolled," or "enrolling" means the process by  
4 which a facial recognition service creates a facial template from one  
5 or more images of an individual and adds the facial template to a  
6 gallery used by the facial recognition service for recognition or  
7 persistent tracking of individuals. It also includes the act of  
8 adding an existing facial template directly into a gallery used by a  
9 facial recognition service.

10 (3) "Facial recognition service" means technology that analyzes  
11 facial features and is used for recognition or persistent tracking of  
12 individuals in still or video images.

13 (4) "Facial template" means the machine-interpretable pattern of  
14 facial features that is extracted from one or more images of an  
15 individual by a facial recognition service.

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

19 (6) "Ongoing surveillance" means tracking the physical movements  
20 of a specified individual through one or more public places over  
21 time, whether in real time or through application of a facial  
22 recognition service to historical records. It does not include a  
23 single recognition or attempted recognition of an individual, if no  
24 attempt is made to subsequently track that individual's movement over  
25 time after they have been recognized.

26 (7) "Persistent tracking" means the use of a facial recognition  
27 service to track the movements of an individual on a persistent basis  
28 without identification or verification of that individual. Such  
29 tracking becomes persistent as soon as:

30 (a) The facial template that permits the tracking is maintained  
31 for more than forty-eight hours after first enrolling that template;  
32 or

33 (b) Data created by the facial recognition service is linked to  
34 any other data such that the individual who has been tracked is  
35 identified or identifiable.

36 (8) "Recognition" means the use of a facial recognition service  
37 to determine whether an unknown individual matches:

38 (a) Any individual who has been enrolled in a gallery used by the  
39 facial recognition service; or

1 (b) A specific individual who has been enrolled in a gallery used  
2 by the facial recognition service.

3 (9) "Serious criminal offense" means any felony under chapter  
4 9.94A RCW, crimes against persons under RCW 9.94A.411, or an offense  
5 enumerated by Title 18 U.S.C. Sec. 2516.

6 NEW SECTION. **Sec. 3.** (1) A state or local government agency  
7 using or intending to develop, procure, or use a facial recognition  
8 service must produce an accountability report for that service. The  
9 report must be clearly communicated to the public at least ninety  
10 days prior to the agency putting the facial recognition service into  
11 operational use, posted on the agency's public web site, and  
12 submitted to the consolidated technology services agency established  
13 in RCW 43.105.006. The consolidated technology services agency must  
14 post each submitted accountability report on its public web site.

15 (2) Each accountability report must include, at minimum, clear  
16 and understandable statements of the following:

17 (a) (i) The name of the facial recognition service, vendor, and  
18 version; and (ii) a description of its general capabilities and  
19 limitations, including reasonably foreseeable capabilities outside  
20 the scope of the proposed use of the agency;

21 (b) (i) The type or types of data inputs that the technology uses;  
22 (ii) how that data is generated, collected, and processed; and (iii)  
23 the type or types of data the system is reasonably likely to  
24 generate;

25 (c) (i) A description of the purpose and proposed use of the  
26 facial recognition service, including what decision or decisions will  
27 be used to make or support it; (ii) whether it is a final or support  
28 decision system; and (iii) its intended benefits, including any data  
29 or research demonstrating those benefits;

30 (d) A clear use and data management policy, including protocols  
31 for the following:

32 (i) How and when the facial recognition service will be deployed  
33 or used and by whom including, but not limited to, the factors that  
34 will be used to determine where, when, and how the technology is  
35 deployed, and other relevant information, such as whether the  
36 technology will be operated continuously or used only under specific  
37 circumstances. If the facial recognition service will be operated or  
38 used by another entity on the agency's behalf, the facial recognition

1 service accountability report must explicitly include a description  
2 of the other entity's access and any applicable protocols;

3 (ii) Any measures taken to minimize inadvertent collection of  
4 additional data beyond the amount necessary for the specific purpose  
5 or purposes for which the facial recognition service will be used;

6 (iii) Data integrity and retention policies applicable to the  
7 data collected using the facial recognition service, including how  
8 the agency will maintain and update records used in connection with  
9 the service, how long the agency will keep the data, and the  
10 processes by which data will be deleted;

11 (iv) Any additional rules that will govern use of the facial  
12 recognition service and what processes will be required prior to each  
13 use of the facial recognition service;

14 (v) Data security measures applicable to the facial recognition  
15 service including how data collected using the facial recognition  
16 service will be securely stored and accessed, if and why an agency  
17 intends to share access to the facial recognition service or the data  
18 from that facial recognition service with any other entity, and the  
19 rules and procedures by which an agency sharing data with any other  
20 entity will ensure that such entities comply with the sharing  
21 agency's use and data management policy as part of the data sharing  
22 agreement; and

23 (vi) The agency's training procedures, including those  
24 implemented in accordance with section 8 of this act, and how the  
25 agency will ensure that all personnel who operate the facial  
26 recognition service or access its data are knowledgeable about and  
27 able to ensure compliance with the use and data management policy  
28 prior to use of the facial recognition service;

29 (e) The agency's testing procedures, including its processes for  
30 periodically undertaking operational tests of the facial recognition  
31 service in accordance with section 6 of this act;

32 (f) A description of any potential impacts of the facial  
33 recognition service on civil rights and liberties, including  
34 potential impacts to privacy and potential disparate impacts on  
35 marginalized communities, and the specific steps the agency will take  
36 to mitigate the potential impacts and prevent unauthorized use of the  
37 facial recognition service; and

38 (g) The agency's procedures for receiving feedback, including the  
39 channels for receiving feedback from individuals affected by the use

1 of the facial recognition service and from the community at large, as  
2 well as the procedures for responding to feedback.

3 (3) Prior to finalizing and implementing the accountability  
4 report, the agency must consider issues raised by the public through:

5 (a) A public review and comment period; and

6 (b) Community consultation meetings during the public review  
7 period.

8 (4) The accountability report must be updated every two years and  
9 each update must be subject to the public comment and community  
10 consultation processes described in this section.

11 (5) An agency seeking to use a facial recognition service for a  
12 purpose not disclosed in the agency's existing accountability report  
13 must first seek public comment and community consultation on the  
14 proposed new use and adopt an updated accountability report pursuant  
15 to the requirements contained in this section.

16 (6) The accountability report required for the facial recognition  
17 matching system authorized in RCW 46.20.037 is due July 1, 2021.

18 NEW SECTION. **Sec. 4.** (1) State and local government agencies  
19 using a facial recognition service are required to prepare and  
20 publish an annual report that discloses:

21 (a) The extent of their use of such services;

22 (b) An assessment of compliance with the terms of their  
23 accountability report;

24 (c) Any known or reasonably suspected violations of their  
25 accountability report, including categories of complaints alleging  
26 violations; and

27 (d) Any revisions to the accountability report recommended by the  
28 agency during the next update of the policy.

29 (2) The annual report must be submitted to the office of privacy  
30 and data protection.

31 (3) All agencies must hold community meetings to review and  
32 discuss their annual report within sixty days of its public release.

33 NEW SECTION. **Sec. 5.** State and local government agencies using  
34 a facial recognition service to make decisions that produce legal  
35 effects concerning individuals or similarly significant effects  
36 concerning individuals must ensure that those decisions are subject  
37 to meaningful human review. Decisions that produce legal effects  
38 concerning individuals or similarly significant effects concerning

1 individuals means decisions that result in the provision or denial of  
2 financial and lending services, housing, insurance, education  
3 enrollment, criminal justice, employment opportunities, health care  
4 services, or access to basic necessities such as food and water.

5 NEW SECTION. **Sec. 6.** Prior to deploying a facial recognition  
6 service in the context in which it will be used, state and local  
7 government agencies using a facial recognition service to make  
8 decisions that produce legal effects on individuals or similarly  
9 significant effect on individuals must test the facial recognition  
10 service in operational conditions. State and local government  
11 agencies must take reasonable steps to ensure best quality results by  
12 following all reasonable guidance provided by the developer of the  
13 facial recognition service.

14 NEW SECTION. **Sec. 7.** (1) A state or local government agency  
15 that deploys a facial recognition service must require a facial  
16 recognition service provider to make available an application  
17 programming interface or other technical capability, chosen by the  
18 provider, to enable legitimate, independent, and reasonable tests of  
19 those facial recognition services for accuracy and unfair performance  
20 differences across distinct subpopulations. However, making such an  
21 application programming interface or other technical capability  
22 available does not require the disclosure of proprietary data, trade  
23 secrets, intellectual property, or other information, or if doing so  
24 would increase the risk of cyberattacks including, without  
25 limitation, cyberattacks related to unique methods of conducting  
26 business, data unique to the product or services, or determining  
27 prices or rates to be charged for services. Such subpopulations are  
28 defined by visually detectable characteristics such as: (a) Race,  
29 skin tone, ethnicity, gender, age, or disability status; or (b) other  
30 protected characteristics that are objectively determinable or self-  
31 identified by the individuals portrayed in the testing dataset. If  
32 the results of the independent testing identify material unfair  
33 performance differences across subpopulations, and the methodology,  
34 data, and results are disclosed in a manner that allows full  
35 reproduction directly to the provider who, acting reasonably,  
36 determines that the methodology and results of that testing are  
37 valid, then the provider must develop and implement a plan to  
38 mitigate the identified performance differences.

1 (2) This section does not apply to the facial recognition  
2 matching system authorized in RCW 46.20.037 under contract as of the  
3 effective date of this section. Upon renewal or extension of the  
4 contract as of the effective date of this section, or upon entering  
5 into a new contract for facial recognition services, the department  
6 of licensing must ensure that the facial recognition service provider  
7 of the system authorized in RCW 46.20.037 fulfills the requirements  
8 of this section.

9 NEW SECTION. **Sec. 8.** State and local government agencies using  
10 a facial recognition service must conduct periodic training of all  
11 individuals who operate a facial recognition service or who process  
12 personal data obtained from the use of a facial recognition service.  
13 The training must include, but not be limited to, coverage of:

14 (1) The capabilities and limitations of the facial recognition  
15 service;

16 (2) Procedures to interpret and act on the output of the facial  
17 recognition service; and

18 (3) To the extent applicable to the deployment context, the  
19 meaningful human review requirement for decisions that produce legal  
20 effects concerning individuals or similarly significant effects  
21 concerning individuals.

22 NEW SECTION. **Sec. 9.** (1) State local and government agencies  
23 must disclose their use of a facial recognition service on a criminal  
24 defendant to that defendant in a timely manner prior to trial.

25 (2) State and local government agencies using a facial  
26 recognition service shall maintain records of their use of the  
27 service that are sufficient to facilitate public reporting and  
28 auditing of compliance with agencies' facial recognition policies.

29 (3) In January of each year, any judge who has issued a warrant  
30 for ongoing surveillance, or an extension thereof, as described in  
31 section 12(1) of this act, that expired during the preceding year, or  
32 who has denied approval of such a warrant during that year shall  
33 report to the Washington state supreme court:

34 (a) The fact that a warrant or extension was applied for;

35 (b) The fact that the warrant or extension was granted as applied  
36 for, was modified, or was denied;

37 (c) The period of ongoing surveillance authorized by the warrant  
38 and the number and duration of any extensions of the warrant;

1 (d) The identity of the applying investigative or law enforcement  
2 officer and agency making the application and the person authorizing  
3 the application; and

4 (e) The nature of the public spaces where the surveillance was  
5 conducted.

6 NEW SECTION. **Sec. 10.** This chapter does not apply to a state or  
7 local government agency that is mandated to use a specific facial  
8 recognition service pursuant to a federal regulation or order.

9 NEW SECTION. **Sec. 11.** (1)(a) A legislative task force on facial  
10 recognition services is established, with members as provided in this  
11 subsection.

12 (i) The president of the senate shall appoint one member from  
13 each of the two largest caucuses of the senate;

14 (ii) The speaker of the house of representatives shall appoint  
15 one member from each of the two largest caucuses of the house of  
16 representatives;

17 (iii) Two representatives from advocacy organizations that  
18 represent individuals or protected classes of communities  
19 historically impacted by surveillance technologies including, but not  
20 limited to, African American, Hispanic American, Native American, and  
21 Asian American communities, religious minorities, protest and  
22 activist groups, and other vulnerable communities;

23 (iv) Two members from law enforcement or other agencies of  
24 government;

25 (v) One representative from a retailer or other company who  
26 deploys facial recognition services in physical premises open to the  
27 public;

28 (vi) Two representatives from companies that develop and provide  
29 facial recognition services; and

30 (vii) Two representatives from universities or research  
31 institutions who are experts in either facial recognition services or  
32 their sociotechnical implications, or both.

33 (b) The task force shall choose two cochairs from among its  
34 legislative membership.

35 (2) The task force shall review the following issues:

36 (a) Provide recommendations addressing the potential abuses and  
37 threats posed by the use of a facial recognition service to civil  
38 liberties and freedoms, privacy and security, and discrimination



1 against vulnerable communities, as well as other potential harm,  
2 while also addressing how to facilitate and encourage the continued  
3 development of a facial recognition service so that individuals,  
4 businesses, government, and other stakeholders in society continue to  
5 utilize its benefits;

6 (b) Provide recommendations regarding the adequacy and  
7 effectiveness of applicable Washington state laws; and

8 (c) Conduct a study on the quality, accuracy, and efficacy of a  
9 facial recognition service including, but not limited to, its  
10 quality, accuracy, and efficacy across different subpopulations.

11 (3) Staff support for the task force must be provided by senate  
12 committee services and the house of representatives office of program  
13 research.

14 (4) Legislative members of the task force are reimbursed for  
15 travel expenses in accordance with RCW 44.04.120. Nonlegislative  
16 members are not entitled to be reimbursed for travel expenses if they  
17 are elected officials or are participating on behalf of an employer,  
18 governmental entity, or other organization. Any reimbursement for  
19 other nonlegislative members is subject to chapter 43.03 RCW.

20 (5) The expenses of the task force must be paid jointly by the  
21 senate and the house of representatives. Task force expenditures are  
22 subject to approval by the senate facilities and operations committee  
23 and the house of representatives executive rules committee, or their  
24 successor committees.

25 (6) The task force shall report its findings and recommendations  
26 to the governor and the appropriate committees of the legislature by  
27 September 30, 2021.

28 (7) This section expires May 1, 2022.

29 NEW SECTION. **Sec. 12.** A new section is added to chapter 9.73  
30 RCW to read as follows:

31 (1) State and local government agencies may not use a facial  
32 recognition service to engage in ongoing surveillance unless the use  
33 is in support of law enforcement activities and the ongoing  
34 surveillance may provide evidence of a serious criminal offense, and  
35 either:

36 (a) A search warrant has been obtained to permit the use of the  
37 facial recognition service for ongoing surveillance; or

38 (b) Where the agency reasonably determines that ongoing  
39 surveillance is necessary to prevent or respond to an emergency

1 involving imminent danger or risk of death or serious physical injury  
2 to a person, but only if written approval is obtained from the  
3 agency's director or the director's designee prior to using the  
4 service. For the purpose of ongoing surveillance, an ex parte order  
5 for a search warrant must be obtained within forty-eight hours after  
6 the emergency surveillance begins. In the absence of an authorizing  
7 order, such use must immediately terminate at the earliest of the  
8 following:

9 (i) The information sought is obtained;

10 (ii) The application for the order is denied; or

11 (iii) When forty-eight hours have lapsed since the beginning of  
12 the emergency surveillance for the purpose of ongoing surveillance.

13 (2) State and local government agencies must not apply a facial  
14 recognition service to any individual based on their religious,  
15 political, or social views or activities, participation in a  
16 particular noncriminal organization or lawful event, or actual or  
17 perceived race, ethnicity, citizenship, place of origin, age,  
18 disability, gender, gender identity, sexual orientation, or other  
19 characteristic protected by law. The prohibition in this subsection  
20 does not prohibit state and local government agencies from applying a  
21 facial recognition service to an individual who happens to possess  
22 one or more of these characteristics where an officer of that agency  
23 holds a reasonable suspicion that that individual has committed, is  
24 committing, or is about to commit a serious criminal offense.

25 (3) State and local government agencies may not use a facial  
26 recognition service to create a record describing any individual's  
27 exercise of rights guaranteed by the First Amendment of the United  
28 States Constitution and by Article I, section 5 of the state  
29 Constitution, unless:

30 (a) Such use is specifically authorized by applicable law and is  
31 pertinent to and within the scope of an authorized law enforcement  
32 activity; and

33 (b) There is reasonable suspicion to believe the individual has  
34 committed, is committing, or is about to commit a serious criminal  
35 offense.

36 (4) Law enforcement agencies that utilize body worn camera  
37 recordings shall comply with the provisions of RCW 42.56.240(14).

1        NEW SECTION.    **Sec. 13.**    Sections 1 through 10 of this act  
2    constitute a new chapter in Title 43 RCW.

--- **END** ---