

SSB 6280 - S AMD 1127

By Senator Nguyen

PULLED 02/19/2020

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

3 "NEW SECTION. **Sec. 1.** The legislature finds that:

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

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

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

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

20 (2) "Enroll," "enrolled," or "enrolling" means the process by
21 which a facial recognition service creates a facial template from one
22 or more images of an individual and adds the facial template to a
23 gallery used by the facial recognition service for recognition or
24 persistent tracking of individuals. It also includes the act of
25 adding an existing facial template directly into a gallery used by a
26 facial recognition service.

27 (3) (a) "Facial recognition service" means technology that
28 analyzes facial features and is used by a state or local government
29 agency for the identification, verification, or persistent tracking
30 of individuals in still or video images.

1 (b) "Facial recognition service" does not include: (i) The
2 analysis of facial features to grant or deny access to an electronic
3 device; or (ii) the use of an automated or semiautomated process for
4 the purpose of redacting a recording for release or disclosure
5 outside the law enforcement agency to protect the privacy of a
6 subject depicted in the recording, if the process does not generate
7 or result in the retention of any biometric data or surveillance
8 information.

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

12 (5) "Identification" means the use of a facial recognition
13 service by a state or local government agency to determine whether an
14 unknown individual matches any individual whose identity is known to
15 the state or local government agency and who has been enrolled by
16 reference to that identity in a gallery used by the facial
17 recognition service.

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

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

28 (8) "Persistent tracking" means the use of a facial recognition
29 service by a state or local government agency to track the movements
30 of an individual on a persistent basis without identification or
31 verification of that individual. Such tracking becomes persistent as
32 soon as:

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

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

1 (9) "Recognition" means the use of a facial recognition service
2 by a state or local government agency to determine whether an unknown
3 individual matches:

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

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

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

11 (11) "Verification" means the use of a facial recognition service
12 by a state or local government agency to determine whether an
13 individual is a specific individual whose identity is known to the
14 state or local government agency and who has been enrolled by
15 reference to that identity in a gallery used by the facial
16 recognition service.

17 NEW SECTION. **Sec. 3.** (1) A state or local government agency
18 using or intending to develop, procure, or use a facial recognition
19 service must produce an accountability report for that service. The
20 report must be clearly communicated to the public at least ninety
21 days prior to the agency putting the facial recognition service into
22 operational use, posted on the agency's public web site, and
23 submitted to the consolidated technology services agency established
24 in RCW 43.105.006. The consolidated technology services agency must
25 post each submitted accountability report on its public web site.

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

28 (a) (i) The name of the facial recognition service, vendor, and
29 version; and (ii) a description of its general capabilities and
30 limitations, including reasonably foreseeable capabilities outside
31 the scope of the proposed use of the agency;

32 (b) (i) The type or types of data inputs that the technology uses;
33 (ii) how that data is generated, collected, and processed; and (iii)
34 the type or types of data the system is reasonably likely to
35 generate;

36 (c) (i) A description of the purpose and proposed use of the
37 facial recognition service, including what decision or decisions will
38 be used to make or support it; (ii) whether it is a final or support

1 decision system; and (iii) its intended benefits, including any data
2 or research demonstrating those benefits;

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

5 (i) How and when the facial recognition service will be deployed
6 or used and by whom including, but not limited to, the factors that
7 will be used to determine where, when, and how the technology is
8 deployed, and other relevant information, such as whether the
9 technology will be operated continuously or used only under specific
10 circumstances. If the facial recognition service will be operated or
11 used by another entity on the agency's behalf, the facial recognition
12 service accountability report must explicitly include a description
13 of the other entity's access and any applicable protocols;

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

17 (iii) Data integrity and retention policies applicable to the
18 data collected using the facial recognition service, including how
19 the agency will maintain and update records used in connection with
20 the service, how long the agency will keep the data, and the
21 processes by which data will be deleted;

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

25 (v) Data security measures applicable to the facial recognition
26 service including how data collected using the facial recognition
27 service will be securely stored and accessed, if and why an agency
28 intends to share access to the facial recognition service or the data
29 from that facial recognition service with any other entity, and the
30 rules and procedures by which an agency sharing data with any other
31 entity will ensure that such entities comply with the sharing
32 agency's use and data management policy as part of the data sharing
33 agreement;

34 (vi) How the facial recognition service provider intends to
35 fulfill security breach notification requirements pursuant to chapter
36 19.255 RCW and how the agency intends to fulfill security breach
37 notification requirements pursuant to RCW 42.56.590; and

38 (vii) The agency's training procedures, including those
39 implemented in accordance with section 8 of this act, and how the
40 agency will ensure that all personnel who operate the facial

1 recognition service or access its data are knowledgeable about and
2 able to ensure compliance with the use and data management policy
3 prior to use of the facial recognition service;

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

7 (f) Information on the facial recognition service's rate of false
8 matches, potential impacts on protected subpopulations, and how the
9 agency will address error rates, determined independently, greater
10 than one percent;

11 (g) A description of any potential impacts of the facial
12 recognition service on civil rights and liberties, including
13 potential impacts to privacy and potential disparate impacts on
14 marginalized communities, and the specific steps the agency will take
15 to mitigate the potential impacts and prevent unauthorized use of the
16 facial recognition service; and

17 (h) The agency's procedures for receiving feedback, including the
18 channels for receiving feedback from individuals affected by the use
19 of the facial recognition service and from the community at large, as
20 well as the procedures for responding to feedback.

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

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

24 (b) Community consultation meetings during the public review
25 period.

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

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

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

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

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

1 (b) An assessment of compliance with the terms of their
2 accountability report;

3 (c) Any known or reasonably suspected violations of their
4 accountability report, including categories of complaints alleging
5 violations; and

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

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

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

12 NEW SECTION. **Sec. 5.** State and local government agencies using
13 a facial recognition service to make decisions that produce legal
14 effects concerning individuals or similarly significant effects
15 concerning individuals must ensure that those decisions are subject
16 to meaningful human review. Decisions that produce legal effects
17 concerning individuals or similarly significant effects concerning
18 individuals means decisions that result in the provision or denial of
19 financial and lending services, housing, insurance, education
20 enrollment, criminal justice, employment opportunities, health care
21 services, or access to basic necessities such as food and water.

22 NEW SECTION. **Sec. 6.** Prior to deploying a facial recognition
23 service in the context in which it will be used, state and local
24 government agencies using a facial recognition service to make
25 decisions that produce legal effects on individuals or similarly
26 significant effect on individuals must test the facial recognition
27 service in operational conditions. State and local government
28 agencies must take reasonable steps to ensure best quality results by
29 following all reasonable guidance provided by the developer of the
30 facial recognition service.

31 NEW SECTION. **Sec. 7.** (1) A state or local government agency
32 that deploys a facial recognition service must require a facial
33 recognition service provider to make available an application
34 programming interface or other technical capability, chosen by the
35 provider, to enable legitimate, independent, and reasonable tests of
36 those facial recognition services for accuracy and unfair performance
37 differences across distinct subpopulations. However, making such an

1 application programming interface or other technical capability
2 available does not require the disclosure of proprietary data, trade
3 secrets, intellectual property, or other information, or if doing so
4 would increase the risk of cyberattacks including, without
5 limitation, cyberattacks related to unique methods of conducting
6 business, data unique to the product or services, or determining
7 prices or rates to be charged for services. Such subpopulations are
8 defined by visually detectable characteristics such as: (a) Race,
9 skin tone, ethnicity, gender, age, or disability status; or (b) other
10 protected characteristics that are objectively determinable or self-
11 identified by the individuals portrayed in the testing dataset. If
12 the results of the independent testing identify material unfair
13 performance differences across subpopulations, and the methodology,
14 data, and results are disclosed in a manner that allows full
15 reproduction directly to the provider who, acting reasonably,
16 determines that the methodology and results of that testing are
17 valid, then the provider must develop and implement a plan to
18 mitigate the identified performance differences.

19 (2) This section does not apply to the facial recognition
20 matching system authorized in RCW 46.20.037 under contract as of the
21 effective date of this section. Upon renewal or extension of the
22 contract as of the effective date of this section, or upon entering
23 into a new contract for facial recognition services, the department
24 of licensing must ensure that the facial recognition service provider
25 of the system authorized in RCW 46.20.037 fulfills the requirements
26 of this section.

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

32 (1) The capabilities and limitations of the facial recognition
33 service;

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

36 (3) To the extent applicable to the deployment context, the
37 meaningful human review requirement for decisions that produce legal
38 effects concerning individuals or similarly significant effects
39 concerning individuals.

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

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

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

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

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

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

18 (d) The identity of the applying investigative or law enforcement
19 officer and agency making the application and the person authorizing
20 the application; and

21 (e) The nature of the public spaces where the surveillance was
22 conducted.

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

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

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

31 (ii) The speaker of the house of representatives shall appoint
32 one member from each of the two largest caucuses of the house of
33 representatives;

34 (iii) Eight representatives from advocacy organizations that
35 represent individuals or protected classes of communities
36 historically impacted by surveillance technologies including, but not
37 limited to, African American, Hispanic American, Native American, and

1 Asian American communities, religious minorities, protest and
2 activist groups, and other vulnerable communities;

3 (iv) Two members from law enforcement or other agencies of
4 government;

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

8 (vi) Two representatives from consumer protection organizations;

9 (vii) Two representatives from companies that develop and provide
10 facial recognition services; and

11 (viii) Two representatives from universities or research
12 institutions who are experts in either facial recognition services or
13 their sociotechnical implications, or both.

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

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

17 (a) Provide recommendations addressing the potential abuses and
18 threats posed by the use of a facial recognition service to civil
19 liberties and freedoms, privacy and security, and discrimination
20 against vulnerable communities, as well as other potential harm,
21 while also addressing how to facilitate and encourage the continued
22 development of a facial recognition service so that individuals,
23 businesses, government, and other stakeholders in society continue to
24 utilize its benefits;

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

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

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

33 (4) Legislative members of the task force are reimbursed for
34 travel expenses in accordance with RCW 44.04.120. Nonlegislative
35 members are not entitled to be reimbursed for travel expenses if they
36 are elected officials or are participating on behalf of an employer,
37 governmental entity, or other organization. Any reimbursement for
38 other nonlegislative members is subject to chapter 43.03 RCW.

39 (5) The expenses of the task force must be paid jointly by the
40 senate and the house of representatives. Task force expenditures are

1 subject to approval by the senate facilities and operations committee
2 and the house of representatives executive rules committee, or their
3 successor committees.

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

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

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

10 (1) State and local government agencies may not use a facial
11 recognition service to engage in ongoing surveillance unless the use
12 is in support of law enforcement activities and the ongoing
13 surveillance may provide evidence of a serious criminal offense, and
14 either:

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

17 (b) Where the agency reasonably determines that ongoing
18 surveillance is necessary to prevent or respond to an emergency
19 involving imminent danger or risk of death or serious physical injury
20 to a person, but only if written approval is obtained from the
21 agency's director or the director's designee prior to using the
22 service. For the purpose of ongoing surveillance, an ex parte order
23 for a search warrant must be obtained within forty-eight hours after
24 the emergency surveillance begins. In the absence of an authorizing
25 order, such use must immediately terminate at the earliest of the
26 following:

27 (i) The information sought is obtained;

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

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

31 (2) State and local government agencies must not apply a facial
32 recognition service to any individual based on their religious,
33 political, or social views or activities, participation in a
34 particular noncriminal organization or lawful event, or actual or
35 perceived race, ethnicity, citizenship, place of origin, age,
36 disability, gender, gender identity, sexual orientation, or other
37 characteristic protected by law. This subsection does not condone
38 profiling including, but not limited to, predictive law enforcement
39 tools. The prohibition in this subsection does not prohibit state and

1 local government agencies from applying a facial recognition service
2 to an individual who happens to possess one or more of these
3 characteristics where an officer of that agency holds a reasonable
4 suspicion that that individual has committed, is committing, or is
5 about to commit a serious criminal offense.

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

11 (a) Such use is specifically authorized by applicable law and is
12 pertinent to and within the scope of an authorized law enforcement
13 activity; and

14 (b) There is reasonable suspicion to believe the individual has
15 committed, is committing, or is about to commit a serious criminal
16 offense.

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

19 (5) A facial recognition service match alone does not constitute
20 reasonable suspicion.

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

SSB 6280 - S AMD 1127
By Senator Nguyen

PULLED 02/19/2020

23 On page 1, line 1 of the title, after "services;" strike the
24 remainder of the title and insert "adding a new section to chapter
25 9.73 RCW; adding a new chapter to Title 43 RCW; creating a new
26 section; and providing an expiration date."

EFFECT: Clarifies the user of a facial recognition service in the
definitions of facial recognition service, persistent tracking, and
recognition.

Exempts services that grant or deny access to an electronic
device or that process for the purpose of redacting a recording from
the definition of facial recognition service.

Provides definitions for identification and verification.

Requires the accountability report to include protocols regarding
security breach notification requirements under current law and

information related to a facial recognition service such as rates of false matches.

Increases the number of representatives from advocacy organizations on the task force from two to eight.

Adds two representatives from consumer protection organizations to the task force.

Specifies that profiling is not condoned and that a facial recognition service match does not constitute reasonable suspicion.

Makes technical corrections.

--- END ---