

ESSB 6280 - H COMM AMD

By Committee on Innovation, Technology & Economic Development

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

3 "NEW SECTION. **Sec. 1.** 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) "Legislative authority" means the respective city or county
19 council, commission, or other body in which legislative powers are
20 vested. For a state agency, "legislative authority" refers to the
21 state legislature.

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

25 (8) "Nonidentifying demographic data" means data that is not
26 linked or reasonably linkable to an identified or identifiable
27 individual, and includes, at a minimum, information about gender,
28 race or ethnicity, age, and location.

29 (9) "Ongoing surveillance" means tracking the physical movements
30 of a specified individual through one or more public places over
31 time, whether in real time or through application of a facial
32 recognition service to historical records. It does not include a
33 single recognition or attempted recognition of an individual, if no
34 attempt is made to subsequently track that individual's movement over
35 time after they have been recognized.

36 (10) "Persistent tracking" means the use of a facial recognition
37 service by a state or local government agency to track the movements
38 of an individual on a persistent basis without identification or
39 verification of that individual. Such tracking becomes persistent as
40 soon as:

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

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

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

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

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

14 (12) "Serious criminal offense" means any offense defined under
15 RCW 9.94A.030 (26), (33), (42), (43), (47), or (56).

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

22 NEW SECTION. **Sec. 3.** (1) A state or local government agency
23 using or intending to develop, procure, or use a facial recognition
24 service must file with a legislative authority a notice of intent to
25 develop, procure, or use a facial recognition service and specify a
26 purpose for which the technology is to be used. A state or local
27 government agency may commence the accountability report required in
28 this section only upon the approval of the notice of intent by the
29 legislative authority.

30 (2) Prior to developing, procuring, or using a facial recognition
31 service, a state or local government agency must produce an
32 accountability report for that service. Each accountability report
33 must include, at minimum, clear and understandable statements of the
34 following:

35 (a) (i) The name of the facial recognition service, vendor, and
36 version; and (ii) a description of its general capabilities and
37 limitations, including reasonably foreseeable capabilities outside
38 the scope of the proposed use of the agency;

1 (b) (i) The type or types of data inputs that the technology uses;
2 (ii) how that data is generated, collected, and processed; and (iii)
3 the type or types of data the system is reasonably likely to
4 generate;

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

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

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

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

24 (iii) Data integrity and retention policies applicable to the
25 data collected using the facial recognition service, including how
26 the agency will maintain and update records used in connection with
27 the service, how long the agency will keep the data, and the
28 processes by which data will be deleted;

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

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

1 (vi) How the facial recognition service provider intends to
2 fulfill security breach notification requirements pursuant to chapter
3 19.255 RCW and how the agency intends to fulfill security breach
4 notification requirements pursuant to RCW 42.56.590; and

5 (vii) The agency's training procedures, including those
6 implemented in accordance with section 8 of this act, and how the
7 agency will ensure that all personnel who operate the facial
8 recognition service or access its data are knowledgeable about and
9 able to ensure compliance with the use and data management policy
10 prior to use of the facial recognition service;

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

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

18 (g) A description of any potential impacts of the facial
19 recognition service on civil rights and liberties, including
20 potential impacts to privacy and potential disparate impacts on
21 marginalized communities, and the specific steps the agency will take
22 to mitigate the potential impacts and prevent unauthorized use of the
23 facial recognition service; and

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

28 (3) Prior to finalizing the accountability report, the agency
29 must:

30 (a) Allow for a public review and comment period;

31 (b) Hold at least three community consultation meetings; and

32 (c) Consider the issues raised by the public through the public
33 review and comment period and the community consultation meetings.

34 (4) The final accountability report must be adopted by a
35 legislative authority in a public meeting before the agency may
36 develop, procure, or use a facial recognition service.

37 (5) The final adopted accountability report must be clearly
38 communicated to the public at least ninety days prior to the agency
39 putting the facial recognition service into operational use, posted
40 on the agency's public web site, and submitted to the consolidated

1 technology services agency established in RCW 43.105.006. The
2 consolidated technology services agency must post each submitted
3 accountability report on its public web site.

4 (6) A state or local government agency seeking to procure a
5 facial recognition service must require vendors to disclose any
6 complaints or reports of bias regarding the service.

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

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

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

17 (10) Except for the facial recognition matching system authorized
18 in RCW 46.20.037, a state or local government agency that is using a
19 facial recognition service as of the effective date of this section
20 must suspend its use of the service until it complies with the
21 requirements of this chapter.

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

25 (a) The extent and effectiveness of their use of such services,
26 including nonidentifying demographic data about individuals subjected
27 to a facial recognition service;

28 (b) An assessment of compliance with the terms of their
29 accountability report;

30 (c) Any known or reasonably suspected violations of their
31 accountability report, including categories of complaints alleging
32 violations; and

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

35 (2) The annual report must be adopted by a legislative authority
36 and submitted to the office of privacy and data protection.

37 (3) All agencies must hold community meetings to review and
38 discuss their annual report within sixty days of its adoption by a
39 legislative authority and public release.

1 NEW SECTION. **Sec. 5.** State and local government agencies using
2 a facial recognition service to make decisions that produce legal
3 effects concerning individuals or similarly significant effects
4 concerning individuals must ensure that those decisions are subject
5 to meaningful human review. Decisions that produce legal effects
6 concerning individuals or similarly significant effects concerning
7 individuals means decisions that result in the provision or denial of
8 financial and lending services, housing, insurance, education
9 enrollment, criminal justice, employment opportunities, health care
10 services, or access to basic necessities such as food and water, or
11 that impact civil rights of individuals.

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

21 NEW SECTION. **Sec. 7.** (1) A facial recognition service provider
22 that provides or intends to provide facial recognition services to
23 state or local government agencies must make available an application
24 programming interface or other technical capability, chosen by the
25 provider, to enable legitimate, independent, and reasonable tests of
26 those facial recognition services for accuracy and unfair performance
27 differences across distinct subpopulations. 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 (3) Nothing in this section requires a state or local government
10 to collect or provide data to a facial recognition service provider
11 to satisfy the requirements in subsection (1) of this section.

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

17 (1) The capabilities and limitations of the facial recognition
18 service;

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

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

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

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

32 (3) In January of each year, any judge who has issued a warrant
33 for ongoing surveillance, or an extension thereof, as described in
34 section 12(1) of this act, that expired during the preceding year, or
35 who has denied approval of such a warrant during that year shall
36 report to the administrator for the courts:

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

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

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

5 (d) The identity of the applying investigative or law enforcement
6 officer and agency making the application and the person authorizing
7 the application; and

8 (e) The nature of the public spaces where the surveillance was
9 conducted.

10 (4) In January of each year, any state or local government agency
11 that has applied for a warrant, or an extension thereof, for ongoing
12 surveillance as described in section 12(1) of this act shall provide
13 to a legislative authority a report summarizing nonidentifying
14 demographic data of individuals named in warrant applications as
15 subjects of ongoing surveillance with the use of a facial recognition
16 service.

17 NEW SECTION. **Sec. 10.** This chapter does not apply to a state or
18 local government agency that is mandated to use a specific facial
19 recognition service pursuant to a federal regulation or order. A
20 state or local government agency must report the mandated use of a
21 facial recognition service to a legislative authority.

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

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

27 (ii) The speaker of the house of representatives shall appoint
28 one member from each of the two largest caucuses of the house of
29 representatives;

30 (iii) Eight representatives from advocacy organizations that
31 represent individuals or protected classes of communities
32 historically impacted by surveillance technologies including, but not
33 limited to, African American, Hispanic American, Native American, and
34 Asian American communities, religious minorities, protest and
35 activist groups, and other vulnerable communities;

36 (iv) Two members from law enforcement or other agencies of
37 government;

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

4 (vi) Two representatives from consumer protection organizations;

5 (vii) Two representatives from companies that develop and provide
6 facial recognition services; and

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

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

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

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

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

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

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

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

35 (5) The expenses of the task force must be paid jointly by the
36 senate and the house of representatives. Task force expenditures are
37 subject to approval by the senate facilities and operations committee
38 and the house of representatives executive rules committee, or their
39 successor committees.

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

4 (7) This section expires September 30, 2022.

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

7 (1) State and local government agencies may not use a facial
8 recognition service to engage in any surveillance, including, but not
9 limited to, engaging in ongoing surveillance, creating a facial
10 template, conducting an identification, starting persistent
11 surveillance, or performing a recognition, without a warrant.

12 (2) State and local government agencies must not apply a facial
13 recognition service to any individual based on their religious,
14 political, or social views or activities, participation in a
15 particular noncriminal organization or lawful event, or actual or
16 perceived race, ethnicity, citizenship, place of origin, immigration
17 status, age, disability, gender, gender identity, sexual orientation,
18 or other characteristic protected by law. This subsection does not
19 condone profiling including, but not limited to, predictive law
20 enforcement tools. The prohibition in this subsection does not
21 prohibit state and local government agencies from applying a facial
22 recognition service to an individual who happens to possess one or
23 more of these characteristics where an officer of that agency holds a
24 reasonable suspicion that that individual has committed, is engaged
25 in, or is about to commit a felony or there is need to invoke their
26 community care-taking function.

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

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

34 (5) A facial recognition service match alone does not constitute
35 reasonable suspicion.

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

EFFECT: The striking amendment makes the following changes to the underlying bill:

(1) Adds definitions of "legislative authority" and "nonidentifying demographic data."

(2) Requires an agency using or intending to develop, procure, or use a facial recognition service to file a notice of intent with a legislative authority.

(3) Requires a legislative authority's approval of the notice of intent before an agency may commence the accountability report.

(4) Specifies that an agency must produce an accountability report prior to developing, procuring, or using a facial recognition service.

(5) Requires an agency to hold at least three community consultation meetings prior to finalizing the accountability report.

(6) Requires a legislative authority to adopt the final accountability report in a public meeting before the agency may develop, procure, or use a facial recognition service.

(7) Provides that an agency seeking to procure a facial recognition service must require vendors to disclose any complaints or reports of bias.

(8) Specifies that an agency that is using a facial recognition service as of the effective date of the bill must suspend its use of the service until it complies with the requirements of the bill.

(9) Requires the annual report to disclose information about the effectiveness of an agency's use of facial recognition services and include nonidentifying demographic data about individuals subjected to facial recognition services.

(10) Requires the annual report to be adopted by a legislative authority.

(11) Modifies the description of decisions that produce legal effects to include decisions that impact civil rights of individuals.

(12) Requires agencies to follow all guidance, rather than all reasonable guidance, provided by the developer of a facial recognition service.

(13) Modifies provisions related to independent testing by requiring facial recognition service providers to make an API or other technical capability available for independent testing.

(14) Removes provisions related to the disclosure of proprietary data and increased risk of cyberattacks.

(15) Specifies that an agency is not required to collect or provide data to a facial recognition service provider in order to satisfy the independent testing requirement.

(16) Requires each agency that has applied for a warrant for ongoing surveillance to provide to a legislative authority a report summarizing nonidentifying demographic data of individuals named in warrant applications as subjects of ongoing surveillance.

(17) Requires an agency to report to a legislative authority any use of a facial recognition service that is mandated by a federal regulation or order.

(18) Removes provisions that specify the circumstances under which agencies may use facial recognition for ongoing surveillance and instead prohibits agencies from using facial recognition for any surveillance without a warrant.

(19) Eliminates the circumstances under which an agency is permitted to use a facial recognition service to create a record describing an individual's exercise of certain constitutional rights.

--- END ---