

ESSB 6280 - H AMD 2097

By Representative Klippert

WITHDRAWN 03/06/2020

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, identifying perpetrators of crime and bringing them to
15 justice, and keeping the public safe.

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

19 (1)(a) "Facial recognition service" means technology that
20 analyzes facial features and is used by a state or local government
21 agency for the identification, verification, or ongoing surveillance
22 of individuals in still or video images.

23 (b) "Facial recognition service" does not include: (i) The
24 analysis of facial features to grant or deny access to a controlled
25 access area or an electronic device or system; (ii) the use of an
26 automated or semiautomated process for the purpose of redacting a
27 recording for release or disclosure outside the law enforcement
28 agency to protect the privacy of a subject depicted in the recording,
29 if the process does not generate or result in the retention of any
30 biometric data or surveillance information; (iii) the analysis of
31 facial features as part of security systems protecting government

1 facilities or property; or (iv) other uses that do not involve the
2 involuntary analysis of the facial features of a member of the
3 general public.

4 (2) "Facial recognition transparency report" means a report
5 developed in accordance with section 3 of this act.

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

9 (4) "Ongoing surveillance" means the continuous tracking of the
10 physical movements of an identified individual through one or more
11 public places for more than forty-eight consecutive hours by law
12 enforcement.

13 NEW SECTION. **Sec. 3.** (1) At least ninety days prior to putting
14 a facial recognition service into operational use for the first time
15 after the effective date of this section, a state or local government
16 agency must produce a facial recognition transparency report. The
17 report must be clearly communicated to the public, posted on the
18 agency's public web site, and submitted to the consolidated
19 technology services agency established in RCW 43.105.006. The
20 consolidated technology services agency must post each submitted
21 transparency report on its public web site.

22 (2) Each facial recognition transparency report must include, at
23 minimum, clear and understandable statements of the following:

24 (a) The name of the facial recognition service, vendor, and
25 version, and a description of its general capabilities and
26 limitations;

27 (b) A description of the purpose and proposed use of the facial
28 recognition service and its intended benefits, including any data or
29 research demonstrating those benefits;

30 (c) A clear use and data management policy;

31 (d) Measures taken to minimize inadvertent collection of
32 additional data beyond the amount necessary for the specific purpose
33 or purposes for which the facial recognition service will be used;

34 (e) Data integrity and retention policies applicable to the data
35 collected using the facial recognition service, including how the
36 agency will maintain and update records used in connection with the
37 service, how long the agency will keep the data, and the processes by
38 which data will be deleted;

1 (f) Any additional rules that will govern use of the facial
2 recognition service;

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

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

10 (3) Prior to finalizing and implementing the facial recognition
11 transparency report, the agency must consider issues raised by the
12 public through:

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

14 (b) Community consultation meetings during the public review
15 period.

16 (4) The agency may update its facial recognition transparency
17 report as it deems necessary and each update must be subject to the
18 public comment and community consultation processes described in this
19 section and submitted to the consolidated technology services agency.

20 (5) The facial recognition transparency report required for any
21 facial recognition system in use as of the effective date of this
22 section is due December 1, 2021.

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

26 (a) A summary of the extent of their use of such services;

27 (b) An assessment of compliance with the provisions of the
28 agency's facial recognition transparency report;

29 (c) Any known violations of the agency's facial recognition
30 transparency report; and

31 (d) Any revisions to the facial recognition transparency report
32 recommended by the agency.

33 (2) All agencies must hold community meetings to review and
34 discuss their annual report within sixty days of its public release.

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

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

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

14 NEW SECTION. **Sec. 7.** (1)(a) A state or local government agency
15 that deploys a facial recognition service must require a facial
16 recognition service provider to either:

17 (i) Make available an application programming interface or other
18 technical capability, chosen by the provider, to enable legitimate,
19 independent, and reasonable tests of those facial recognition
20 services for accuracy and unfair performance differences across
21 distinct subpopulations. However, making such an application
22 programming interface or other technical capability available does
23 not require the disclosure of proprietary data, trade secrets,
24 intellectual property, or other information, or if doing so would
25 increase the risk of cyber attacks including, without limitation,
26 cyber attacks related to unique methods of conducting business, data
27 unique to the product or services, or determining prices or rates to
28 be charged for services. Such subpopulations are defined by visually
29 detectable characteristics such as: (A) Race, skin tone, ethnicity,
30 gender, age, or disability status; or (B) other protected
31 characteristics that are objectively determinable among the
32 individuals portrayed in the testing data set: Provided, however,
33 that such characteristics are characteristics that the facial
34 recognition service provider claims the technology is capable of
35 detecting, and are characteristics that the state or local government
36 agency intends to detect with its facial recognition service; or

37 (ii) Submit the service to the national institute of standards
38 and technology for review and testing.

1 (b) If the results of the independent testing identify material
2 unfair performance differences across subpopulations, and the
3 methodology, data, and results are disclosed in a manner that allows
4 full reproduction directly to the provider who, acting reasonably,
5 determines that the methodology and results of that testing are
6 valid, then the provider must develop and implement a plan to
7 mitigate the identified performance differences.

8 (2) This section does not apply to any facial recognition service
9 in use as of the effective date of this section. Upon renewal or
10 extension of any contract as of the effective date of this section,
11 or upon entering into a new contract for facial recognition services,
12 the state or local government agency must ensure that the facial
13 recognition service provider fulfills the requirements of this
14 section.

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

20 (1) The capabilities and limitations of the facial recognition
21 service;

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

24 (3) To the extent applicable to the deployment context, the
25 meaningful human review requirement for decisions that produce legal
26 effects concerning individuals.

27 NEW SECTION. **Sec. 9.** (1) State and local government agencies
28 must disclose to a criminal defendant evidence gathered through the
29 use of a facial recognition service that has been used, or is
30 intended to be used against the defendant in the current criminal
31 proceeding in a timely manner prior to trial.

32 (2) State and local government agencies using a facial
33 recognition service shall maintain records of their use of the
34 service that are sufficient to facilitate the annual reporting under
35 section 4 of this act.

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

4 NEW SECTION. **Sec. 11.** A new section is added to chapter 9.73
5 RCW to read as follows:

6 (1) State and local government agencies may not use a facial
7 recognition service:

8 (a) In a manner that disturbs a person's private affairs, or
9 invades their home, without authority of law;

10 (b) Without a bona fide criminal justice purpose;

11 (c) Without reasonable suspicion that a criminal offense has been
12 committed, is being committed, or is about to be committed; or

13 (d) To engage in ongoing surveillance unless the use is in
14 support of law enforcement activities and there is reasonable
15 suspicion to believe that an individual has committed, is engaged in,
16 or is about to commit, a criminal offense or there is a need by law
17 enforcement to invoke their community caretaking function, and
18 either:

19 (i) A court order has been obtained to permit the use of the
20 facial recognition service for ongoing surveillance; or

21 (ii) Where the agency reasonably determines that an exigent
22 circumstance exists, and an appropriate court order is obtained as
23 soon as reasonably practicable. In the absence of an authorizing
24 order, such use must immediately terminate at the earliest of the
25 following:

26 (A) The information sought is obtained;

27 (B) The application for the order is denied; or

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

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

1 characteristics where an officer of that agency holds a reasonable
2 suspicion that that individual has committed, is engaged in, or is
3 about to commit a criminal offense or there is need to invoke their
4 community caretaking function.

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

10 (a) Such use is pertinent to and within the scope of an
11 authorized law enforcement activity; and

12 (b) There is reasonable suspicion to believe the individual has
13 committed, is engaged in, or is about to commit a criminal offense or
14 there is need to invoke their community caretaking function.

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

17 (5) State and local law enforcement agencies may not use the
18 results of a facial recognition service as the sole basis to
19 establish probable cause in a criminal investigation. The results of
20 a facial recognition service may be used in conjunction with other
21 information and evidence lawfully obtained by a law enforcement
22 officer to establish probable cause in a criminal investigation.

23 (6) State and local law enforcement agencies may not use a facial
24 recognition service to identify an individual based on a sketch or
25 other manually produced image.

26 (7) State and local law enforcement agencies may not
27 substantively manipulate an image for use in a facial recognition
28 service in any manner not consistent with the facial recognition
29 service provider's intended use and training.

30 NEW SECTION. **Sec. 12.** Sections 1 through 10 of this act
31 constitute a new chapter in Title 43 RCW."

32 Correct the title.

EFFECT: (1) Modifies legislative findings to specify that
beneficial uses include identifying perpetrators of crime.

(2) Modifies definitions of facial recognition service and
ongoing surveillance. Adds a definition of facial recognition
transparency report. Deletes the definition of persistent tracking
and others.

(3) Requires transparency reports (rather than accountability reports), and specifies their content, review, and timing.

(4) Modifies annual reports to include summaries of uses of facial recognition services, as well as compliance with, known violations of, and recommended revisions to, transparency reports. Does not require submission to the Office of Privacy and Data Protection.

(5) Narrows requirements for human review and operational testing. Requires human review of decisions producing legal effects, but not decisions producing "similarly significant effects concerning individuals."

(6) Modifies independent testing requirements. Authorizes government agencies to submit facial recognition services to the National Institute of Standards & Technology (in addition to making an Application Programming Interface (API) available). Modifies API provisions to describe certain characteristics as those that providers claim the technology is capable of detecting and that government agencies intend to detect. Does not require testing of services already in use.

(7) Modifies disclosure and report requirements. Requires timely disclosure to criminal defendants of the evidence gathered through facial recognition services for use in current criminal proceedings. Does not require reports of ongoing surveillance to the state Administrator for the Courts.

(8) Prohibits use of facial recognition services without authority of law, a bona fide criminal justice purpose, or without reasonable suspicion of a criminal offense. Also prohibits the use of services to engage in ongoing surveillance unless certain conditions are met, including that there is reasonable suspicion of a criminal offense (rather than probable cause of a felony).

(9) Modifies permitted and prohibited applications. Permits applying facial recognition services in specified circumstances where there is reasonable suspicion of a criminal offense (rather than a felony).

(10) Specifies that government agencies may not use results of facial recognition services as the sole basis to establish probable cause. Prohibits using services to identify individuals based on sketches and manipulating images for use inconsistent with the service provider's intended use and training.

(11) Strikes the Legislative Task Force on Facial Recognition Services.

--- END ---