ESSB 6280 - H AMD TO H AMD (H-5405.2/20) **2127**
By Representative Klippert

NOT ADOPTED 03/06/2020

On page 1, line 14, after "crime," insert "identifying perpetrators of crime and bringing them to justice,"

On page 1, beginning on line 18, after "(1)" strike all material through "(3)" on line 27

Renumber the remaining subsections consecutively and correct any internal references accordingly.

Beginning on page 1, line 29, after "or" strike all material through "individuals." on page 7, line 11 and insert "ongoing surveillance of individuals in still or video images.

(b) "Facial recognition service" does not include: (i) The analysis of facial features to grant or deny access to a controlled access area or an electronic device or system; (ii) the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information; (iii) the analysis of facial features as part of security systems protecting government facilities or property; or (iv) other uses that do not involve the involuntary analysis of the facial features of a member of the general public.

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

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

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

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

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

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

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

(c) A clear use and data management policy;

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

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

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

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

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

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

(a) A public review and comment period; and

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

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

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

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

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

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

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

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

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

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

On page 7, beginning on line 15, after "individuals" strike all material through "individuals" on line 16

On page 7, line 19, after "all" insert "reasonable"

Beginning on page 7, line 21, strike all of section 7 and insert the following:

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

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

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

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

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

On page 8, beginning on line 18, after "individuals" strike all material through "individuals" on line 19

Beginning on page 8, line 20, strike all of sections 9 through 18 and insert the following:

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

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

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

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

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

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

(b) Without a bona fide criminal justice purpose;

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

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

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

(ii) Where the agency reasonably determines that an exigent circumstance exists, and an appropriate court order is obtained as soon as reasonably practicable. In the absence of an authorizing

order, such use must immediately terminate at the earliest of the following:

(A) The information sought is obtained;

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

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

(2) State and local government agencies must not apply a facial recognition service to any individual based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law. This subsection does not condone profiling. The prohibition in this subsection does not prohibit state and local government agencies from applying a facial recognition service to an individual who possesses one or more of these characteristics where an officer of that agency holds a reasonable suspicion that that individual has committed, is engaged in, or is about to commit a criminal offense or there is need to invoke their community caretaking function.

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

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

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

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

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

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

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

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

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. Does not require adoption by legislative authorities.

(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 impacting civil rights or 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 relating to intellectual property and testing for unfair performance. 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 on warrants and ongoing surveillance to the state Administrator for the Courts and legislative authorities.

(8) Modifies warrant requirements. Prohibits the use of facial recognition services without authority of law, a bona fide criminal justice purpose, or without reasonable suspicion of a criminal offense (rather than without warrants). Also prohibits the use for ongoing surveillance unless in support of law enforcement activities, with reasonable suspicion of a criminal offense, and with either a court order or a determination of exigent circumstances (and a court order as soon as reasonably practicable).

(9) Modifies permitted and prohibited applications. Permits applying facial recognition services to individuals where an officer holds a reasonable suspicion of a criminal offense (rather than a felony) or there is need to invoke community caretaking. Also permits the use to create records of constitutional rights if such use is pertinent and within the scope of authorized law enforcement activity

and there is reasonable suspicion of a criminal offense or need to invoke community caretaking. Does not prohibit applying facial recognition services to individuals based on their immigration status.

(10) 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 Facial Recognition Task Force to be established by the Ruckelshaus Center.

(12) Removes provisions related to the use of facial recognition services by controllers and processors.

--- END ---