SSB 6280 - S AMD **1155**
By Senator Nguyen

ADOPTED 02/19/2020

Strike everything after the enacting clause and insert the following:

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

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

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

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

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

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

(3)(a) "Facial recognition service" means technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking 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 an electronic device; or (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.

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

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

(6) "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.

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

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

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

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

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

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

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

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

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

NEW SECTION. **Sec. 3.** (1) A state or local government agency using or intending to develop, procure, or use a facial recognition service must produce an accountability report for that service. The report must be clearly communicated to the public at least ninety days prior to the agency putting the facial recognition service into operational use, 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 accountability report on its public web site.

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

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

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

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

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

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

(ii) Any 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;

(iii) 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;

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

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

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

(vii) The agency's training procedures, including those implemented in accordance with section 8 of this act, and how the agency will ensure that all personnel who operate the facial recognition service or access its data are knowledgeable about and

able to ensure compliance with the use and data management policy prior to use of the facial recognition service;

(e) 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;

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

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

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

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

(6) The accountability report required for the facial recognition matching system authorized in RCW 46.20.037 is due July 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) The extent of their use of such services;

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

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

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

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

(3) 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 or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review. Decisions that produce legal effects concerning individuals or similarly significant 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.

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

NEW SECTION. **Sec. 7.** (1) A state or local government agency that deploys a facial recognition service must require a facial recognition service provider to 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 cyberattacks including, without limitation, cyberattacks 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 or self-identified by the individuals portrayed in the testing dataset. 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 the facial recognition matching system authorized in RCW 46.20.037 under contract as of the effective date of this section. Upon renewal or extension of the contract as of the effective date of this section, or upon entering into a new contract for facial recognition services, the department of licensing must ensure that the facial recognition service provider of the system authorized in RCW 46.20.037 fulfills the requirements of this section.

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

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

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

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

NEW SECTION. **Sec. 9.** (1) State and local government agencies must disclose their use of a facial recognition service on a criminal defendant to that defendant 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 public reporting and auditing of compliance with agencies' facial recognition policies.

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

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

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

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

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

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

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

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

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

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

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

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

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

(vi) Two representatives from consumer protection organizations;

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

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

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

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

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

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

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

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

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

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

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

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

(7) This section expires May 1, 2022.

NEW SECTION. **Sec. 12.** 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 to engage in ongoing surveillance unless the use is in support of law enforcement activities and there is probable cause to believe that an individual has committed, is engaged in, or is about to commit, a felony or there is a need by law enforcement to invoke their community care-taking function, and either:

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

(b) 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:

(i) The information sought is obtained;

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

(iii) 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 including, but not limited to, predictive law enforcement tools. The prohibition in this subsection does not prohibit state and local government agencies from applying a facial recognition service to an individual who happens to possess 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 felony or there is need to invoke their community care-taking 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 specifically authorized by applicable law and 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 felony or there is need to invoke their community care-taking function.

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

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

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

SSB 6280 - S AMD **1155**
By Senator Nguyen

ADOPTED 02/19/2020

On page 1, line 1 of the title, after "services;" strike the remainder of the title and insert "adding a new section to chapter 9.73 RCW; adding a new chapter to Title 43 RCW; creating a new 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.

Revises the definition of serious criminal offense.

Clarifies that judges shall submit required reports to the administrator for the courts.

Clarifies that a facial recognition service may not be used for ongoing surveillance unless there is probable cause to believe that an individual has committed, is engaged in, or is about to commit a felony or there is a need by law enforcement to invoke their community care-taking function.

Clarifies permitted uses of a facial recognition service by requiring a court order or determination of exigent circumstances.

Clarifies that prohibitions do not prohibit application of a facial recognition service if there is reasonable suspicion that an individual has committed, is engaged in, or is about to commit a felony or there is need to invoke community care-taking functions.

--- END ---