<u>**ESSB 6280**</u> - H AMD **2120**
By Representative Entenman

ADOPTED AS AMENDED 03/06/2020

Strike everything after the enacting clause and insert the following:

"<u>NEW SECTION.</u> **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.

<u>NEW SECTION.</u> **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) "Legislative authority" means the respective city, county, or other local governmental agency's council, commission, or other body in which legislative powers are vested. For a port district, the legislative authority refers to the port district's port commission. For an airport established pursuant to chapter 14.08 RCW and operated by a board, the legislative authority refers to the airport's board. For a state agency, "legislative authority" refers to the technology services board created in RCW 43.105.285.

(7) "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.

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

(9) "Ongoing surveillance" means using a facial recognition service to track 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.

(10) "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.

(11) "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.

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

(13) "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 file with a legislative authority a notice of intent to develop, procure, or use a facial recognition service and specify a purpose for which the technology is to be used. A state or local government agency may commence the accountability report required in this section only upon the approval of the notice of intent by the legislative authority.

(2) Prior to developing, procuring, or using a facial recognition service, a state or local government agency must produce an accountability report for that service. 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 the accountability report, the agency must:

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

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

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

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

(5) The final adopted accountability 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.

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

(7) 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.

(8) A state or local government agency that is using a facial recognition service as of the effective date of this section must suspend its use of the service until it complies with the requirements of this chapter.

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 and effectiveness of their use of such services, including nonidentifying demographic data about individuals subjected to a facial recognition service;

(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 adoption by a legislative authority and 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, or that impact civil rights of individuals.

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 guidance provided by the developer of the facial recognition service.

NEW SECTION. **Sec. 7.** (1)(a) A facial recognition service provider that provides or intends to provide facial recognition services to state or local government agencies must 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. Such subpopulations are defined by visually detectable characteristics such as: (i) Race, skin tone, ethnicity, gender, age, or disability status; or (ii) 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, the provider must develop and implement a plan to mitigate the identified performance differences.

(b) Making an application programming interface or other technical capability does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data. Providers bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing.

(2) Nothing in this section requires a state or local government to collect or provide data to a facial recognition service provider to satisfy the requirements in subsection (1) 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 the use of a facial recognition service to engage in any surveillance, or an extension thereof, as described in section 13(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 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.

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

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, or that are undertaken through partnership with a federal agency to fulfill a congressional mandate. A state or local government agency must report the mandated use of a facial recognition service to a legislative authority.

NEW SECTION. **Sec. 11.** (1) Any person who has been subjected to a facial recognition service in violation of this chapter or about whom information has been obtained, retained, accessed, or used in violation of this chapter, may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this chapter.

(2) A court shall award costs and reasonable attorneys' fees to a prevailing plaintiff in an action brought under subsection (1) of this section.

NEW SECTION. **Sec. 12.** (1)(a) The William D. Ruckelshaus center must establish a facial recognition task force, 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) 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.

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

(5) This section expires September 30, 2022.

NEW SECTION. **Sec. 13.** 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 any surveillance including, but not limited to, engaging in ongoing surveillance, creating a facial template, conducting an identification, starting persistent surveillance, or performing a recognition, without a warrant, unless exigent circumstances exist.

(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, immigration status, 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.

(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.

(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.

NEW SECTION. **Sec. 14.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Consumer" means a natural person who is a Washington resident.

(2) "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

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

(4) "Facial recognition service" means technology that analyzes facial features and is used for the identification, verification, or persistent tracking of consumers in still or video images.

(5) "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.

(6) "Identification" means the use of a facial recognition service by a controller to determine whether an unknown consumer matches any consumer whose identity is known to the controller and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

(7) "Meaningful human review" means review or oversight by one or more individuals who are trained in accordance with section 15(8) of this act and who have the authority to alter the decision under review.

(8) "Persistent tracking" means the use of a facial recognition service to track the movements of a consumer on a persistent basis without identification or verification of that consumer. Such tracking becomes persistent as soon as:

(a) The facial template that permits the tracking uses a facial recognition service for more than forty-eight hours after the first enrolling of that template; or

(b) The data created by the facial recognition service in connection with the tracking of the movements of the consumer are linked to any other data such that the consumer who has been tracked is identified or identifiable.

(9) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person.

"Personal data" does not include deidentified data or publicly available information.

(10) "Processor" means a natural or legal person who processes personal data on behalf of a controller.

(11) "Recognition" means the use of a facial recognition service to determine whether:

(a) An unknown consumer matches any consumer who has been enrolled in a gallery used by the facial recognition service; or

(b) An unknown consumer matches a specific consumer who has been enrolled in a gallery used by the facial recognition service.

(12) "Verification" means the use of a facial recognition service by a controller to determine whether a consumer is a specific consumer whose identity is known to the controller and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

NEW SECTION. **Sec. 15.** (1)(a) Processors that provide facial recognition services must make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations. Such subpopulations are defined by visually detectable characteristics, such as (i) race, skin tone, ethnicity, gender, age, or disability status, or (ii) other protected characteristics that are objectively determinable or self-identified by the individuals portrayed in the testing dataset. If the results of that independent testing identify material unfair performance differences across subpopulations, the processor must develop and implement a plan to mitigate the identified performance differences. Nothing in this subsection prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.

(b) Making an application programming interface or other technical capability does not require processors to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data. Processors bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing.

(2) Processors that provide facial recognition services must provide documentation that includes general information that:

(a) Explains the capabilities and limitations of the services in plain language; and

(b) Enables testing of the services in accordance with this section.

(3) Processors that provide facial recognition services must prohibit by contract the use of facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.

(4) Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public that includes, at minimum, the following:

(a) The purpose or purposes for which the facial recognition service is deployed; and

(b) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to, a link to any applicable online notice, terms, or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.

(5) Controllers must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premise open to the public.

(6) Controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.

(7) Prior to deploying a facial recognition service in the context in which it will be used, controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must test the facial recognition service in operational conditions. Controllers must take commercially reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the facial recognition service.

(8) Controllers using a facial recognition service must conduct periodic training of all individuals that operate a facial recognition service or that process personal data obtained from the

use of facial recognition services. Such training shall include, but not be limited to, coverage of:

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

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

(c) The meaningful human review requirement for decisions that produce legal effects on consumers or similarly significant effects on consumers, to the extent applicable to the deployment context.

(9) Controllers shall not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency, except when such disclosure is:

(a) Pursuant to the consent of the consumer to whom the personal data relates;

(b) Required by federal, state, or local law in response to a warrant;

(c) Necessary to prevent or respond to an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the controller; or

(d) To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec. 2258A.

(10) Voluntary facial recognition services used to verify an aviation passenger's identity in connection with services regulated by the secretary of transportation under Title 49 U.S.C. Sec. 41712 and exempt from state regulation under Title 49 U.S.C. Sec. 41713(b)(1) are exempt from this section. Images captured by an airline must not be retained for more than twenty-four hours and, upon request of the attorney general, airlines must certify that they do not retain the image for more than twenty-four hours. An airline facial recognition service must disclose and obtain consent from the customer prior to capturing an image.

NEW SECTION. **Sec. 16.** (1) Any person who has been subjected to a facial recognition service in violation of this chapter, or about whom information has been obtained, retained, accessed, or used in violation of this chapter, may institute proceedings in any court of competent jurisdiction to obtain injunctive relief or declaratory relief, or to recover actual damages, but not less than statutory damages of seven thousand five hundred dollars per violation, whichever is greater.

(2) A court shall award costs and reasonable attorneys' fees to a prevailing plaintiff in an action brought under subsection (1) of this section.

NEW SECTION. **Sec. 17.** Nothing in this act applies to the use of a facial recognition matching system by the department of licensing pursuant to RCW 46.20.037.

NEW SECTION. **Sec. 18.** (1) Sections 1 through 11 and 17 of this act constitute a new chapter in Title 43 RCW.

(2) Sections 14 through 16 of this act constitute a new chapter in Title 19 RCW."

Correct the title.

EFFECT: (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) Removes the requirement to update the accountability report every two years.

(9) 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.

(10) 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.

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

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

(13) Specifies that the independent testing requirement does not require providing an API in a manner that would increase the risk of cyberattacks or disclosing proprietary data.

(14) 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.

(15) Expands the judicial report requirement to include applications for warrants for the use of a facial recognition service to engage in any surveillance, rather than applications for warrants for ongoing surveillance.

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

(17) Exempts from the requirements of the bill the use of a facial recognition service undertaken through partnership with a federal agency to fulfill a congressional mandate.

(18) Requires an agency to report to a legislative authority any mandated use of a facial recognition service.

(19) 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, unless exigent circumstances exist.

(20) Removes provisions related to the circumstances under which an agency may apply a facial recognition service to an individual who happens to possess one or more of the protected characteristics.

(21) 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.

(22) Prohibits the use of the results of a facial recognition service as the sole basis to establish probable cause instead of providing that a facial recognition match alone does not constitute reasonable suspicion.

(23) Permits agencies to use the results of a facial recognition service in conjunction with other lawfully obtained evidence to establish probable cause.

(24) Adds enforcement provisions for the use of facial recognition services by agencies.

(25) Modifies the legislative task force provisions by directing the William D. Ruckelshaus Center to convene a facial recognition task force and by removing provisions related to staff support and expenses of the task force.

(26) Exempts from the requirements of the bill the statutorily authorized use of a facial recognition matching system by the Department of Licensing and removes corresponding references.

(27) Sets forth requirements for controllers and processors that use facial recognition services, including third-party testing of the services for accuracy and unfair performance; developing and implementing a plan to address identified performance differences; consumer consent prior to enrolling an image in a facial recognition service; and meaningful human review when using facial recognition services to make decisions that produce legal effects or similarly significant effects on consumers.

(28) Prohibits controllers from knowingly disclosing personal data obtained from a facial recognition service to law enforcement, except when specified conditions apply.

(29) Exempts from the controller and processor requirements the voluntary facial recognition services used to verify an aviation

passenger's identity in connection with services regulated by certain federal laws.

(30) Adds enforcement provisions for the use of facial recognition services by controllers and processors.

(31) Adds definitions related to provision and use of facial recognition services by controllers and processors.

--- END ---