Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Innovation, Technology & Economic Development Committee

ESSB 6280

Brief Description: Concerning the use of facial recognition services.

Sponsors: Senate Committee on Environment, Energy & Technology (originally sponsored by Senators Nguyen, Carlyle, Wellman, Salomon, Lovelett, Das, Randall, Pedersen, Wilson, C. and Hunt).

Brief Summary of Engrossed Substitute Bill

- Sets forth specific requirements for the use of facial recognition services by state and local government agencies, including accountability report, annual report, operational testing, independent testing, training, and meaningful human review.
- Prohibits state and local agencies from using a facial recognition service for ongoing surveillance, unless specified conditions are met, and either a court order is obtained or the agency reasonably determines that exigent circumstances exist and an appropriate court order is obtained as soon as reasonably practicable.
- Prohibits state and local agencies from applying a facial recognition service based on certain protected characteristics or creating a record describing any individual's exercise of certain constitutional rights.
- Specifies disclosure and reporting requirements.
- Creates a legislative task force on facial recognition.

Hearing Date: 2/26/20

Staff: Yelena Baker (786-7301).

Background:

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

Facial Recognition.
Facial recognition is one of several biometric technologies which identify or verify individuals by measuring and analyzing their physiological or behavioral characteristics. Facial recognition generally works by detecting a human face, extracting it from the rest of the scene, and measuring the numerous distinguishable landmarks that make up facial features, such as the distance between the eyes or the shape of the cheekbones. A numerical code called a faceprint or a facial template is then created to represent the measured face in a database.

In a process known as "one-to-one" matching, facial recognition can confirm that a photo matches a different photo of the same person in a database. "One-to-one" matching is commonly used for verification purposes, such as unlocking a smartphone or checking a passport. A "one-to-many" matching process compares a photo of an unknown person to a database of known people and may be used to identify a person of interest.

Facial recognition systems can generate two types of errors: false positives (generating an incorrect match) or false negatives (not generating a match where one exists). The more similar the environments in which the images are compared, the better a facial recognition system will perform, particularly in a "one-to-many" matching process.

Facial recognition is used in a variety of consumer and business applications, including safety and security, secure access, marketing, and customer service. In the public sphere it is more commonly used for law enforcement and security purposes. Additionally, many states, including Washington, use facial recognition matching systems to verify the identity of an applicant for a driver's license or identification card to determine whether the person has been issued a driver's license or identification card under a different name.

State Law Regarding Biometric Identifiers.
A state agency is prohibited from obtaining a biometric identifier without providing notice that clearly specifies the purpose and use of the identifier and obtaining consent specific to the terms of the notice. A state agency that obtains biometric identifiers must minimize the review and retention of biometric identifiers and establish security policies to ensure the integrity and confidentiality of biometric identifiers. A state agency may only use a biometric identifier consistent with the terms of the notice and consent and is prohibited from selling a biometric identifier. Biometric identifiers collected by a state agency may not be disclosed under the Public Records Act.

"Biometric identifier" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry. "Biometric identifier" excludes information derived from certain sources, such as demographic data, physical descriptions, or photographs.

Consolidated Technology Services.
The Consolidated Technology Services (CTS) agency, also known as WaTech, supports state agencies as a centralized provider and procurer of certain information technology (IT) services. Within the CTS, the Office of the Chief Information Officer (OCIO) has certain primary duties related to state government IT, which include establishing statewide enterprise architecture and standards for consistent and efficient operation.

Office of Privacy and Data Protection.
Within the OCIO, the Office of Privacy and Data Protection (OPDP) was created in 2016 to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection. The primary duties of the OPDP with respect to state agencies include conducting privacy reviews and trainings, coordinating data protection, and articulating privacy principles and best policies.

Summary of Bill:

Specific requirements and limitations are set forth for the use of facial recognition services by state and local government agencies.

"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.

"Facial recognition service" does not include:
- the analysis of facial features to grant or deny access to an electronic device; or
- 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.

Accountability Reports.
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 accountability report must include, at a minimum:
- the name of a facial recognition service and a description of its general capabilities and limitations;
- the type or types of data inputs that the facial recognition service uses;
- a description of the purpose and proposed use of the facial recognition service;
- a clear use and data management policy;
- the agency's testing procedures;
- information on the facial recognition service's rate of false matches, potential impacts on protected subpopulations, and how the agency will address certain error rates;
- a description of any potential impacts of the facial recognition service on privacy, civil rights and liberties, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the facial recognition service; and
- the agency's procedures for receiving and responding to feedback from individuals affected by the use of the facial recognition service and from the community at large.

Prior to finalizing and implementing the accountability report, the agency must consider issues raised by the public through a public review and comment period and community consultation meetings. The report must be clearly communicated to the public at least 90 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 for posting on its public web site.

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. The accountability report must be updated every two years, and each update must be subject to the public comment and community consultation processes.

Annual Reports.
A state or local government agency using a facial recognition service must prepare and publish an annual report that discloses:

- the extent of the agency's use of such services;
- an assessment of compliance with the terms of the agency's accountability report;
- any known or reasonably suspected violations of the agency's accountability report; and
- any recommended revisions to the accountability report.

The annual report must be submitted to the Office of Privacy and Data Protection, and the agency must hold community meetings to review and discuss the report within 60 days of its public release.

Meaningful Human Review.
A state or local government agency 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.

Operational Testing.
Prior to deploying a facial recognition service, a state or local government agency using the service to make decisions that produce legal effects on individuals or similarly significant effect on individuals must test the service in operational conditions. An agency must take reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the facial recognition service.

Independent Testing.
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 (API) or other technical capability to enable legitimate, independent, and reasonable tests of the facial recognition service for accuracy and unfair performance differences across distinct subpopulations. However, making API 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.

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.

Training.
A state or local government agency 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 minimum training requirements include the coverage of the capabilities and limitations of the facial recognition service and the meaningful human review requirement.

Limitations on the Use of Facial Recognition Services.
A state or local government agency 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 court order has been obtained to permit the use of the facial recognition service for ongoing surveillance; or
- 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, the agency's use of a facial recognition service must immediately terminate at the earliest of the following:

- the information sought is obtained;
- the application for the order is denied; or
- when 48 hours have lapsed since the beginning of the emergency surveillance for the purpose of ongoing surveillance.

An agency may not apply a facial recognition service to any individuals based on certain characteristics, such as religious or political views and activities, participation in a particular noncriminal organization or lawful event, race, age, citizenship or other characteristic protected by law. This prohibition does not prohibit an agency 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.

An agency may not use a facial recognition service to create a record describing any individual's exercise of the rights guaranteed by the First Amendment of the U.S. Constitution and by Article I, section 5 of the state Constitution, unless:

- such use is specifically authorized by applicable law and is pertinent to and within scope of an authorized law enforcement activity; and
- 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.

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

Disclosures and Reports.
A state or local government agency must disclose its use of a facial recognition service on a criminal defendant to that defendant in a timely manner prior to trial.

An agency using a facial recognition service shall maintain records of its use of the service to facilitate public reporting and auditing of compliance with the agency's facial recognition policies.

In January of each year, any judge who has issued a warrant for ongoing surveillance must report to the state Supreme Court certain information regarding the warrants, including whether the warrant was granted, modified, or denied, the period of ongoing surveillance authorized by the warrant, and the nature of the public spaces where the surveillance was conducted.

Exemptions.
The bill 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.

Legislative Task Force on Facial Recognition.
A legislative task force on facial recognition technology is established to:

- provide recommendations addressing the potential abuses and threats posed by the use of facial recognition, while also addressing how to facilitate and encourage the continued development of the technology so that the society continues to utilize its benefits;
- provide recommendations regarding the adequacy and effectiveness of applicable Washington state laws; and
- conduct a study on the quality, accuracy, and efficacy of facial recognition.

The task force is composed of:

- four legislative members;
- eight representatives from advocacy organizations that represent consumers or communities historically impacted by surveillance technologies;
- two members of from law enforcement or other government agencies;
- one representative from a company that deploys facial recognition in physical premises open to public;
- two representatives from consumer protection organizations;
- two representatives from companies that develop and provide facial recognition services; and
- two representatives from universities or research institutions who are experts in facial recognition or its sociotechnical implications, or both.

By September 30, 2021, the task force must submit a report of its findings and recommendations to the Governor and the appropriate committees of the Legislature.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.