FINAL BILL REPORT
ESSB 6280

PARTIAL VETO
C 257 L 20
Synopsis as Enacted

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).

Senate Committee on Environment, Energy & Technology
House Committee on Innovation, Technology & Economic Development
House Committee on Appropriations

Background: Facial Recognition in General. Facial recognition is a type of biometric technology that provides a way to establish or verify the identify of natural person based on one or more physical or behavioral characteristics and is used in various applications such as security, law enforcement, banking, and retail. Examples of physical characteristics are face, fingerprint, and iris images. An example of a behavioral characteristic is an individual's signature.

Facial recognition technology compares an individual’s facial features to available images for identification or authentication. Facial detection technology determines whether the image contains a face. Facial analysis technology aims to identify attributes such as gender, age, or emotion from detected faces.

Current State Laws. *Biometric Identifiers.* Unless authorized by law, state agencies may not collect, capture, purchase or otherwise obtain a biometric identifier without first providing notice and obtaining the individual's consent. Agencies that obtain any biometric identifier must establish certain security policies and meet certain requirements regarding the use, storage, sale, and sharing of such information.

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, or scan of hand or face geometry. Exceptions are identified such as when information is derived from photographs, demographic data, or physical descriptions such as height, weight, hair color, or eye color.

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 Matching System. The Department of Licensing (DOL) is authorized to implement a facial recognition matching system for all driver licenses, permits, and identicards to determine whether the person has been issued identification under a different name or names. System, notice, and security requirements are specified.

Facial recognition matching system means a system that compares the biometric template derived from an image of an applicant or holder of a driver's license, permit, or identicard with the biometric templates derived from the images in DOL's negative file.

State Agencies. The Consolidated Technology Services (CTS) agency supports state agencies as a centralized provider and procurer of information technology services. Within CTS, the Office of the Chief Information Officer (OCIO) has primary duties related to information technology for state government, which include establishing statewide enterprise architecture and standards for consistent and efficient operation. The Technology Services Board (TSB), which is also created within CTS, has several powers and duties related to information services, which include reviewing and approving standards and policies developed by the OCIO, providing oversight of major information technology projects, and approving contracts for services and activities specified under current law.

Summary: Accountability Report. A state or local government agency (agency) using or intending to develop, procure, or use a service must file with a legislative authority a notice of intent to develop, procure, or use a facial recognition service (service) and specify a purpose for which the service is to be used. After submitting the notice and prior to developing, procuring, or using a service, an agency must produce an accountability report for that service. Each accountability report must include certain statements such as a description of the proposed use of the service, information on the service's rate of false matches, data security measures, and procedures regarding testing and channels for receiving feedback.

Each accountability report must be subject to a public review period and be updated every two years. The report must be posted on the agency's website and submitted to a legislative authority for posting to its public website.

Legislative authority means the respective city, county, or other local government agency's council, commission, or other body in which legislative powers are vested. The legislative authority for a port district refers to the port district's port commission; an airport established pursuant to current law and operated by a board refers to the airport's board; and a state agency refers to the TSB.

Meaningful Human Review. Agencies using a service to make decisions that produce legal effects or similarly significant effects concerning individuals must ensure those decisions are subject to meaningful human review. Decisions that produce legal effects or similarly significant effects concerning individuals means decisions resulting in the provision or denial of financial and lending services, housing, insurance, education enrollment, employment opportunities, health care services, or access to basic necessities such as food and water, or that impact civil rights of individuals.

Independent Testing. An agency must require a service provider to make available an application programming interface (API) to enable independent testing for accuracy and unfair performance differences across distinct subpopulations. Making available an API does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data. If 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 within 90 days of receipt of such results. For purposes of mitigating the identified performance differences, the methodology and data used in the independent testing must be disclosed to the provider in a manner that allows full reproduction.

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

Training. An agency using a service must conduct periodic training of all individuals who operate a service or who process personal data obtained from the use of a service. Minimum training requirements are specified.

Prohibitions. An agency may not use a service to engage in ongoing surveillance, conduct real-time or near-real time identification, or start persistent tracking unless:

- a warrant is obtained;
- exigent circumstances exist; or
- a court order is obtained for the sole purpose of locating or identifying a missing person, or identifying a deceased person.

In addition, an agency may not:

- apply a service to any individual based on certain characteristics protected by law; or
- use a service to create a record describing any individual's exercise of rights guaranteed by the First Amendment of the U.S. Constitution and by Article I, section 5 of the state Constitution.

A law enforcement agency may not:

- use the results of a service as the sole basis to establish probable cause in a criminal investigation—results may be used in conjunction with other information lawfully obtained;
- use a service to identify an individual based on a sketch or manually produced image; or
- substantively manipulate an image for use in a service in a manner not consistent with the service provider's intended use and training.

Exemptions. This act does apply to an agency that:

- is mandated to use a specific service pursuant to a federal regulation or order; or
- uses a service in association with a federal agency to verify the identity of individuals presenting themselves for travel in an airport or seaport.

An agency must report the use of a service pursuant to an exemption to a legislative authority.

Nothing in this act applies to use of a facial recognition matching system by DOL authorized under current law.

Disclosure and Records. Agencies must disclose their use of a service on a criminal defendant to that defendant in a timely manner prior to trial. Agencies using a service shall maintain records of their use of a service to facilitate public reporting and auditing of compliance with the agency's service policies.

Any judge who has issued a warrant for ongoing surveillance shall report to the state supreme court information regarding the warrants, such as the fact that a warrant or extension was applied for, the period of ongoing surveillance, and the nature of the public spaces where the surveillance was conducted.

Any agency that has applied for a warrant for the use of a service to engage in ongoing surveillance, conduct real-time or near real-time identification, or starts persistent tracking must provide a legislative authority with a report summarizing nonidentifying demographic data of individuals named in warrant applications.

Votes on Final Passage:

Senate	30	18	
House	63	33	(House amended)
			(Senate refused to concur/asked House to recede)
			(House insisted/asked Senate for conference)

Conference Committee

			(Conference report not adopted by Senate/conference reappointed)
House	53	43	
Senate	27	21	

Effective: July 1, 2021

Partial Veto Summary:

- Removed a Facial Recognition Task Force.