SENATE BILL REPORT
ESSB 6280

As Passed Senate, February 19, 2020

Title: An act relating to the use of facial recognition services.

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 History:
Committee Activity: Environment, Energy & Technology: 1/15/20, 1/23/20 [DPS, DNP, w/ oRec].
Floor Activity:
Passed Senate: 2/19/20, 30-18.

Brief Summary of Engrossed First Substitute Bill

- Requires state or local government agencies (agencies) to develop an accountability report and an annual report that meet certain requirements on the use of a facial recognition service (service).
- Specifies agency requirements regarding public notification, testing prior to deployment, independent testing for accuracy across distinct subpopulations, and service operator training.
- Prohibits an agency from using a service for ongoing surveillance, unless in support of law enforcement and there is probable cause and either pursuant to a search warrant or the agency reasonably determines that an exigent circumstance exists and an appropriate court order is obtained.
- Specifies disclosure and record keeping requirements.
- Establishes a facial recognition task force.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Majority Report: That Substitute Senate Bill No. 6280 be substituted therefor, and the substitute bill do pass.

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.

Signed by Senators Carlyle, Chair; Lovelett, Vice Chair; Das, Hobbs, Liias, McCoy, Nguyen, Stanford and Wellman.

Minority Report: Do not pass.
Signed by Senators Brown, Rivers and Short.

Minority Report: That it be referred without recommendation.
Signed by Senators Ericksen, Ranking Member; Fortunato, Assistant Ranking Member, Environment.

Staff: Angela Kleis (786-7469)

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. 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.

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. Within the OCIO, the Office of Privacy and Data Protection (OPDP) serves as a central point of contact for state agencies on policy matters involving data privacy and data protection.

Summary of Engrossed First Substitute Bill: Accountability Report. Agencies using or intending to develop, procure, or use a service 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 CTS for posting to its public website.

Annual Report. Agencies using a service must publish an annual report disclosing:
- the extent of their use of such services;
- an assessment of compliance with the terms of their accountability report;
- any known or reasonably suspected violations of their accountability report; and
- any recommended revisions to the accountability report.

The annual report must be submitted to the OPDP. All agencies must hold community meetings to review their annual report within 60 days of its public release.

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.

Independent Testing. Agencies must require a service provider to make available an application programming interface to enable independent testing for accuracy and unfair performance differences across distinct subpopulations. However, making available an application programming interface for tests does not require disclosure of certain information such as proprietary data, or if doing so would increase the risk of cyberattacks. If results of the independent testing identify material unfair performance difference across subpopulations and those results are validated, then the provider must develop and implement a plan to mitigate the identified performance differences.

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

Training. Agencies 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. Agencies may not use a service for 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 search warrant has been obtained; or
- where the agency reasonably determines that an exigent circumstance exists, and an appropriate court order is obtained as soon as reasonably practicable.

Agencies must not apply a service to any individual based on certain characteristics protected by law. This prohibition does not prohibit agencies from applying a service to an individual who happens to possess one or more characteristics where an officer of that agency holds a reasonable suspicion that 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.

Agencies may not 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, 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.

Exemption. This act does apply to a state or local government agency mandated to use a specific facial recognition service pursuant to a federal regulation or order.

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.

Task Force. A legislative task force on facial recognition services is established with the purpose of:

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

Task force membership is composed of legislative members and representatives from advocacy organizations, government agencies, retailers that deploy services in public spaces, companies that develop and provide services, consumer protection organizations, and research institutions with expertise on services. The task force shall submit a report of its findings and recommendations to the Governor and the Legislature by September 30, 2021.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: Yes.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Original Bill: *The committee recommended a different version of the bill than what was heard.* PRO: We need accountability measures in place to serve our communities. This is thoughtful regulation of the government's use of facial recognition technology by requiring transparency, judicial oversight, and community engagement.

CON: We suggest a moratorium on the government use of the technology until certain requirements are met. This seeks to regulate technology before allowing communities to decide if they want the technology used in the first place. The reporting requirements are a deterrent to the use of certain technology. There are concerns with provisions regarding a search warrant.

OTHER: We want to make sure that the testing requirements do not release any proprietary information and that this is not in conflict with the body camera statute.

Persons Testifying: PRO: Senator Joe Nguyen, Prime Sponsor; Ryan Harkins, Microsoft.

CON: Cameron Cantrell, University of Washington School of Law; Jevan Hutson, University of Washington School of Law; Jennifer Lee, ACLU of Washington; James McMahan, Washington Association Sheriffs and Police Chiefs; Mark Streuli, Motorola Solutions.

OTHER: Russell Brown, Executive Director, WAPA; Michael Transue, AXON.

Persons Signed In To Testify But Not Testifying: No one.