HOUSE BILL REPORT
ESSB 6280

As Reported by House Committee On:
Innovation, Technology & Economic Development

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:
Innovation, Technology & Economic Development: 2/26/20, 2/28/20 [DPA].

Brief Summary of Engrossed Substitute Bill
(As Amended by Committee)

- Sets forth specific requirements for the use of facial recognition services by state and local government agencies, including accountability report, annual reports, operational testing, independent testing, training, and meaningful human review.
- Prohibits state and local agencies from using a facial recognition service for any surveillance, from applying a facial recognition service based on certain protected characteristics, and from 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.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: Do pass as amended. Signed by 7 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Entenman, Slatter, Tarleton and Wylie.

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.

Minority Report: Do not pass. Signed by 2 members: Representatives Boehnke, Assistant Ranking Minority Member; Van Werven.

Staff: Yelena Baker (786-7301).

Background:

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 Amended 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.

Notice of Intent.
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 and specify a purpose for which the technology is to be used. The legislative authority must approve the notice of intent before the agency may commence an accountability report.

Accountability Reports.
Prior to developing, procuring, or using a facial recognition service, a state or local government agency 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:
- allow for a public review and comment period;
- hold at least three community consultation meetings; and
- consider issues raised by the public through a public review and comment period and community consultation meetings.

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. 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 and effectiveness of the agency's use of such services, including nonidentifying demographic data about individuals subjected to a facial recognition service;
- 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 adopted by a legislative authority and submitted to the Office of Privacy and Data Protection. The agency must hold community meetings to review and discuss the report within 60 days of its adoption by a legislative authority and 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, access to basic necessities such as food and water, or that impact civil rights of individuals.

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 guidance provided by the developer of the facial recognition service.

Independent Testing.
A facial recognition service provider that provides or intends to provide facial recognition services to a state or local government agency must 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.

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.

An agency is not required to collect or provide data to a facial recognition service provider to satisfy the independent testing requirements.

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.
With the exception of the statutorily authorized use of facial recognition matching system by the Department of Licensing, 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 the bill.

A state or local government agency may not use a facial recognition service to engage in any surveillance without a warrant.

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 immigration status, 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 United States Constitution and by Article I, section 5 of the state Constitution.

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.

In January of each year, any agency that has applied for a warrant for ongoing surveillance must provide to a legislative authority a report summarizing nonidentifying demographic data of individuals named in the warrant applications as subject of ongoing surveillance with the use of a facial recognition service.

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. An agency must report the mandated use of a facial recognition service to a legislative authority.

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 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.

Amended Bill Compared to Engrossed Substitute Bill:

Regarding accountability reports, the amended bill:
- 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;
- requires a legislative authority's approval of the notice of intent before an agency may commence the accountability report;
- specifies that an agency must produce an accountability report prior to developing, procuring, or using a facial recognition service;
- requires an agency to hold at least three community consultation meetings prior to finalizing the accountability report;
- 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; and
- provides that an agency seeking to procure a facial recognition service must require vendors to disclose any complaints or reports of bias.

Regarding annual reports, the amended bill:
- 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; and
- requires the annual report to be adopted by a legislative authority.

Regarding meaningful human review, the amended bill:
- modifies the description of decisions that produce legal effects to include decisions that impact civil rights of individuals.

Regarding independent testing requirements, the amended bill:
- modifies provisions related to independent testing by requiring facial recognition service providers to make an API or other technical capability available for independent testing;
- removes provisions related to the disclosure of proprietary data and increased risk of cyberattacks; and
- 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.

Regarding limitations on the use of facial recognition, the amended bill:

- 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;
- 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; and
- 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.

Regarding disclosures and reports, the amended bill:
- requires each agency that has applied for a warrant for ongoing surveillance to provide to a legislative authority a report summarizing nonidentifying demographic data of individuals named in warrant applications as subjects of ongoing surveillance; and
- requires an agency to report to a legislative authority any use of a facial recognition service that is mandated by a federal regulation or order.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) Strong moral guardrails are required for facial recognition technology. Last year, the Legislature considered but did not pass a moratorium on facial recognition, so a lot of time and effort went into this bill because it is important to get this right.

This bill is informed by numerous stakeholder conversations and other policy proposals in this area. The potential benefits of facial recognition should not be discounted, and the potential harms should not be ignored. This bill allows beneficial uses to continue while putting appropriate safeguards in place to protect against potential harms. There are many examples where thoughtful regulation has improved markets for both customers and producers.

(Opposed) Facial recognition is like plutonium—limited beneficial uses, but toxic and extremely dangerous otherwise. A moratorium on the use of this technology should be in place until the legislative task force comes back with its report.

Some aspects of the bill are really good, but overall the protections are nowhere near strong enough. The bill relies on transparency and reporting requirements, but does not provide any oversight or consequences for failure to report problems or to report at all, which creates opportunities for law enforcement to expand unlawful surveillance. The bill focuses heavily

on the process and ignores the rights. Nothing in the bill discusses secondary uses of data or prohibits matching camera footage to personally identifiable information. Additional language is needed to protect our rights in public spaces and in our interactions with governmental agencies.

The independent testing requirement ignores intersectional biases and does not specify who approves the bias mitigation plan or what happens if mitigation is insufficient. Huge loopholes would allow companies to prevent effective testing, as they have already done with other algorithmic issues.

Wrongful convictions based on bad identification disproportionately affect communities of color. Facial recognition technology exacerbates this issue because its rates of error in identifying people of color is 100 times higher than when identifying white people. Facial recognition also creates a huge confirmation bias.

The bill puts weak restrictions on just one narrow surveillance use of facial recognition and allows broad use of the technology in support of law enforcement activities. Even if facial recognition operates perfectly, the widespread surveillance it creates poses great threats to constitutionally protected rights and civil liberties. Numerous community groups—Japanese Americans, Muslims, trans and gender nonconforming individuals, and immigrant communities—have testified to long having been subject to surveillance and asked for the opportunity to truly decide if, not just how, facial recognition should be used. By pushing for weak regulations that do not threaten the bottom line, the industry hopes to create a façade of responsibility and avoid the real debate about whether this technology should be allowed at all.

The bill empowers corporations and not communities to set the terms of how facial recognition is used. Independent testing requirements intend to address issues of bias, but requiring this testing while using, rather than prior to using, this technology will allow for ongoing experimentation, and marginalized communities will be the ones most impacted.

This bill restricts law enforcement's ability to enforce public safety laws. Law enforcement should not be able to use facial recognition absent reasonable suspicion that a crime has occurred or is about to occur. Law enforcement should not use facial recognition information by itself as the basis for probable cause.

It is a mistake to cast all facial recognition technology as surveillance technology. When used safely and responsibly, facial recognition technology makes everyone safer. The industry has a moral obligation that no technology is used for unethical or discriminatory purposes. Some provisions of the bill could actually curtail a range of beneficial uses. The bill provides an exemption for use related to unlocking electronic devices; a similar exemption should be added in for one-to-one verifications for people who opt into this use of facial recognition. This would not have any privacy or civil liberties impact, but would allow users to securely access government buildings or authenticate their identity for other purposes.

The independent testing requirement unfairly disadvantages small developers because most of them work with programs designed for government use and do not make their technology

publicly available. They should have the option to satisfy the testing requirement by participating in the testing conducted by the National Institute of Standards and Technology.

(Other) Government agencies should not be required to collect or provide data to third parties, so additional clarification regarding the independent testing requirement is needed.

Persons Testifying: (In support) Senator Nguyen, prime sponsor; and Irene Plenefisch, Microsoft Corporation.

(Opposed) David Montes, Washington Defenders Association and Washington Association of Criminal Defense Lawyers; Jenifer Lee, American Civil Liberties Union of Washington; Mckenna Lux, Council on American-Islamic Relations, Washington; Jonathan Pincus, Indivisible Plus: Washington State; Deborah Pierce; James McMahan, Washington Association Sheriffs and Police Chiefs; and Jake Parker, Security Industry Association.

(Other) Beau Perschbacher, Department of Licensing.

Persons Signed In To Testify But Not Testifying: None.