HOUSE BILL REPORT
HB 2856

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

Title: An act relating to a moratorium on facial recognition technology.

Brief Description: Concerning a moratorium on facial recognition technology.

Sponsors: Representatives Entenman, Morgan and Santos.

Brief History:
Committee Activity:
Innovation, Technology & Economic Development: 1/31/20, 2/4/20 [DPS].

Brief Summary of Substitute Bill

- Prohibits the use of facial recognition technology by state and local government agencies until July 1, 2023.
- Prohibits the installation or operation of any equipment that incorporates facial recognition in places of public accommodation until July 1, 2023.
- Creates a joint legislative task force on facial recognition to review existing research, document potential threats, and provide recommendations regarding appropriate regulation of facial recognition.

HOUSE COMMITTEE ON INNOVATION, TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Hudgins, Chair; Kloba, Vice Chair; Smith, Ranking Minority Member; Boehnke, Assistant Ranking Minority Member; Entenman, Slatter, Tarleton, Van Werven and Wylie.

Staff: Yelena Baker (786-7301).

Background:

Facial Recognition.

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 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.

Regulation of Biometric Identifiers.

In 2017 two Washington laws regulating the collection and use of biometric identifiers were enacted: one applies to state agencies and the other to any person or business that enrolls biometric identifiers in a database for commercial purposes.

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.

A person or business may not enroll a biometric identifier in a database for a commercial purpose, without providing notice, obtaining consent, or providing a mechanism to prevent subsequent use. A biometric identifier enrolled or obtained for a commercial purpose may not be used or disclosed in a way inconsistent with the original terms under which it was provided, unless new consent is obtained. The sale, lease, or disclosure of a biometric identifier for a commercial purpose, without the individual's consent, is prohibited except in certain circumstances, such as when it is necessary in providing a product or service sought by the individual or required under a court order. A person or business in possession of biometric identifiers enrolled for a commercial purpose must guard against unauthorized access and adhere to retention limitations.

The definition of "biometric identifier" in both statutes includes data based on an individual's biological characteristics, such as a fingerprint, voiceprint, or scan of hand or face geometry, and excludes data from photographs.

Washington Law Against Discrimination.
The Washington Law Against Discrimination prohibits discrimination based on protected characteristics in places of public accommodation. Protected characteristics include a person's race, religion, national origin, sex or sexual orientation, honorably discharged veteran or military status, the presence of any sensory, mental or physical disability, or the use of a trained dog guide or service animal. A place of public accommodation means any place of public resort, accommodation, assemblage, or amusement. Places of public accommodations generally include restaurants, hotels, stores, shopping malls, movie theaters, concert halls, arenas, parks, fairs, arcades, libraries, schools, government offices, and hospitals.

Consumer Protection Act.
Under the state's Consumer Protection Act (CPA), a variety of business practices are declared unlawful. These practices include engaging in unfair methods of competition and unfair or deceptive acts or practices in the conduct of commerce and monopolizing trade or commerce. A person injured by a violation of the CPA may bring an action for injunctive relief and the recovery of actual damages and reasonable attorneys' fees. Recovery may also include triple damages, in some circumstances. In addition, the CPA allows the Attorney General to bring a CPA action in the name of the state or on behalf of persons residing in the state. An action by the Attorney General may seek to prevent or restrain violations of the act and may seek restoration for persons injured by violation of the CPA.

Summary of Substitute Bill:

Government Use of Facial Recognition.
Until July 1, 2023, state and local government agencies are prohibited from obtaining, retaining, requesting, accessing, or using any facial recognition technology or any information obtained from or by use of facial recognition technology. Information obtained from or by the use of facial recognition may not be received as evidence in any trial or other proceeding before a court or other authority subject to the jurisdiction of Washington.

Inadvertent or unintentional receipt, access, or use of facial recognition information is not a violation of the moratorium if:

- the information was not requested or solicited by an agency; and
- the information is permanently deleted upon discovery.

The moratorium on government use of facial recognition does not apply to the use of facial recognition by the Department of Licensing for purposes of a facial recognition matching system to verify the identity of an applicant for or holder of a driver's license, permit, or identification card. The moratorium does not apply to the use of facial recognition for the purpose of redacting a recording for release or disclosure outside a law enforcement agency to protect the privacy of a subject in the recording, provided that this use of facial recognition does not result in the retention of any biometric data or surveillance information.

A person injured by the violations of these provisions may institute proceedings for injunctive relief, declaratory relief, a writ of mandate, or an action to recover actual damages.

Facial Recognition in Places of Public Accommodation.
Until July 1, 2023, it is prohibited to operate or install any equipment incorporating facial recognition in places of public accommodation, as defined in the Washington Law Against Discrimination.

Violations of these provisions are enforceable under the Consumer Protection Act and subject to civil penalties and statutory damages.

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

- review existing research on the accuracy and efficacy of facial recognition technology;
- document the potential threats posed to civil liberties, privacy, and other potential harm; and
- provide recommendations regarding appropriate regulation of facial recognition technology.

The task force is composed of:

- four legislative members;
- 15 representatives from advocacy organizations that represent consumers or communities historically impacted by surveillance technologies;
- one member of law enforcement;
- one representative from a company that deploys facial recognition in physical premises open to public;
- one representative from a company that develops and provides facial recognition services; and
- two representatives from universities or research institutions who are experts in facial recognition or technology ethics, 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.

Substitute Bill Compared to Original Bill:

The substitute bill adds an exemption for the use of facial recognition for the purpose of redacting a recording for release or disclosure outside a law enforcement agency to protect the privacy of a subject in the recording.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

Effective Date of Substitute 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) A moratorium on facial recognition is appropriate because facial recognition is not accurate in identifying certain people. Facial recognition amplifies existing biases and may be used in ways that are fundamentally unfair. Surveillance impacts marginalized communities the most, and facial recognition poses a greater surveillance threat, particularly because its use is largely undetectable. If left unregulated or inadequately regulated, facial recognition will allow the government and the private sector to track people's movements and associations in ways that threaten the right to privacy, due process, freedom of association, and freedom of expression. Facial recognition technology will improve with time, but it should not be improved at the expense of the people who suffer the greatest harm from its use. Community organizations should be included in any discussion of the future use of facial recognition technology.

(Opposed) There are legitimate uses of facial recognition technology, and imposing a moratorium will eliminate this technology. There is room for agreement on how facial recognition should be used and what standards should apply. No technology is perfect, and human review should always be required. Facial recognition helps solve serious crimes. Law enforcement is trained to treat a facial recognition match as an investigatory lead, like an anonymous tip. The bill should exempt the use of facial recognition to redact the faces of children or victims of crimes from police video footage. Redacting this footage without facial recognition would result in a significantly increased workload. The membership of the task force to study the issues related to facial recognition should be more balanced.

Persons Testifying: (In support) Representative Entenman, prime sponsor; and Eric Gonzalez Alfaro, American Civil Liberties Union of Washington.

(Opposed) Michael Transue, Axon; James McMahan, Washington Association Sheriffs and Police Chiefs; Mark Streuli, Motorola Solutions Inc; and Robert Battles, Association of Washington Business.

Persons Signed In To Testify But Not Testifying: None.