Washington Facial Recognition Law FAQ

June 2020

SECURITY INDUSTRY ASSOCIATION

On March 31, 2020, Washington Gov. Jay Inslee signed into law legislation (SB 6280) that requires state and local agencies, including law enforcement, that use or plan to use facial recognition technologies to meet certain reporting and deployment requirements. This FAQ is intended to help both agencies and vendors in the state understand the law's requirements, with the caveats that ambiguities remain and additional legislative and/or regulatory changes and clarifications are possible. This document should not be regarded as legal advice, and the guidance of qualified legal counsel should be sought as needed.

Who is covered by the law?

The law covers state and local agencies, including law enforcement, that use or plan to use facial recognition technology. No private sector users are covered.

When does the law become effective?

The law is scheduled to take effect in July 2021.

Does the law ban the use of facial recognition technology?

No, the law does not ban the use of facial recognition by state and local agencies, though it does prohibit certain uses that would generally be regarded as inconsistent with civil liberties and equality under the law. Agencies may not apply facial recognition based on an individual's race, gender, ethnicity or other characteristic protected by law, or a person's religious, political or social views or participation in noncriminal organizations or events. In addition, the technology may not be used to create a record of a person's exercise of his or her First Amendment rights.

Does the law restrict uses of facial recognition technology?

Yes. If facial recognition is to be used "to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking," then one of three conditions must be met: a warrant is obtained, exigent circumstances exist or a court order authorizes the technology's use for the identification of a missing or deceased person. The definitions included in the law provide additional guidance:

- "Ongoing surveillance" includes both real-time tracking of the "physical movements of a specified individual through one or more public places over time" and the application of facial recognition to recorded video for that purpose. It specifically excludes "a single recognition or attempted recognition of an individual, if no attempt is made to subsequently track that individual's movement," but the law's limitation on "real-time or near real-time identification" appears to disallow even a single recognition in the absence of a warrant, exigent circumstances or a court order.
- "Persistent tracking" involves using a surveillance system "to track the movements of an individual on a persistent basis without identification or verification of that individual." Facial recognition – technology that determines the identity of individuals – requires an enrollment process to create a photo database against which video images are compared. However, face *detection* and similar analytics may provide the ability to detect that a human face is present, create a template of a selected face – without identification – and use that template to track a person's movements. If this template

is maintained for more than 48 hours or is combined with other data that enables the person to be identified, then the rules regarding persistent tracking apply.

What *can* facial recognition be used for by government agencies?

The law aims to prohibit only those "uses that threaten our democratic freedoms and put our civil liberties at risk." It states that, in accordance with specified procedures, "state and local government agencies may use facial recognition services to locate or identify missing persons, and identify deceased persons, including missing or murdered indigenous women, subjects of Amber alerts and silver alerts, and other possible crime victims, for the purposes of keeping the public safe."

Also, the legislation exempts certain uses. An agency does not have to comply with the law's mandates if:

- It is the state Department of Licensing, which was previously authorized by the legislature to implement a facial recognition system.
- The facial recognition system being used is under a contract that was in place when the law went into effect. The agency will, however, be required to comply with the law when it renews the contract or enters into a new one.
- It is required by a federal mandate to use a specific facial recognition system.
- It uses facial recognition in partnership with a federal agency at an airport or seaport. In this case, the agency must report the use to a legislative authority.

Regulations – and probably case law – will likely provide clearer guidance regarding allowable uses.

Does the law affect the use of government and law enforcement video cameras in public places?

If the video collected by cameras in public places is not processed by facial recognition algorithms – and, in the overwhelming majority of cases, it is not – then the law likely has no impact on the use of those cameras. As noted above, though, some cameras have a face detection analytic, and if this is used for the purpose of tracking individuals – even if they are not identified – then the restriction concerning "persistent tracking" may apply.

What are the requirements concerning facial recognition deployment and use?

When a facial recognition system is used "to make decisions that produce legal effects concerning individuals," an agency must make those decisions subject to human review. "Legal effects" are defined as including "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, or that impact civil rights of individuals." In addition, such a system must be tested in operational conditions before it is deployed and the agency "must take reasonable steps to ensure best quality results."

Agencies must require vendors to include an API or other mechanism that will enable independent testing of the system's accuracy across "distinct subpopulations." If the testing identifies unfair performance differences, the provider must mitigate those differences within 90 days.

Also, agencies must conduct periodic training of all people who use the system or process data obtained by the system; maintain records "that are sufficient to facilitate public reporting and auditing"; and annually report to a legislative authority on the demographic data of people who were named in warrants for facial recognition surveillance. The law also establishes reporting requirements for judges who issue warrants for facial recognition surveillance.

Some additional rules apply primarily to law enforcement. Facial recognition results may not be used as the sole basis to establish probable cause in a criminal investigation (though it can be used in conjunction with other evidence); facial recognition may not be used to identify someone based on a sketch; law enforcement "may not substantively manipulate an image for use in a facial recognition service"; and the use of facial recognition must be disclosed to criminal defendants "in a timely manner prior to trial."

What are the law's reporting requirements?

The law establishes multiple reporting requirements for agencies when renewing facial recognition contracts or entering into new ones. An agency must:

- File a notice of intent with a legislative authority that includes specifying the purpose for which the technology is to be used.
- Prior to deployment, produce an "accountability report" that includes certain details about the system, including, but not limited to, technological information, descriptions of the planned implementation, the use and data management policies, testing procedures and statistics on false positive rates.
- Make the accountability report available to the public for a comment period and hold at least three community meetings about it before it is finalized.
- Release the final accountability report to the public at least 90 days prior to the facial recognition system being deployed.
- Update the accountability report every two years.
- Require vendors to disclose any complaints or reports of bias.
- Update the accountability report and seek public comment anytime a previously undeclared use is added.

Did the law create a task force to study facial recognition uses?

No. While the bill, as passed by the legislature, included language that would have created a facial recognition task force, Gov. Inslee vetoed that section because of a lack of funding. He recommended "that the Legislature engage the Ruckelshaus Center [at the University of Washington and Washington State University] in preparing a situation assessment that would inform policy recommendations on facial recognition technologies. Such an assessment would answer many questions about how best to proceed and could better inform the creation of a task force in a subsequent legislative session."

The SIA Data Privacy Advisory Board provides information and best practices to help SIA members handle sensitive data in a safe, secure and responsible manner in order to protect the personally identifiable information of their employees, partners and customers from potential breaches, respect privacy rights and meet emerging compliance demands.