FACIAL RECOGNITION PRIVACY PROTECTION ACT
SB476 / HB1578
Summary
SECTION-BY-SECTION

Section 1	
	Commercial Law Article **The following sections set rules for the commercial use of facial recognition services**
Definitions **14-4201**	Provides the definitions of key terms.
Scope **14-4202**	Specifies the sections that apply to legal entities conducting business with residents of the state.
Legislative Findings **14-4203**	• Recognizes that the use of facial recognition by the private sector and government agencies presents both benefits and risks. • States that legislation is needed to establish safeguards that will allow use of the technology in beneficial ways while prohibiting uses that threaten privacy and our civil liberties.

Controllers and Processor Obligations
14-4204
	Provides rules for controllers (users) and processors (providers) of facial recognition services.
	<u>Requirements for processors</u>:
	• Make available an application programming interface (API) or other technical capability for testing by third parties for accuracy and bias.
	• Mitigate any unfair performance identified.
	• Explain the capabilities and limitations of the technology.
	• Prohibit the use of the technology in ways that unlawfully discriminate.
	<u>Requirements for controllers</u>:
	• Provide notice that facial recognition is being used.
	• Include in the notice –
	  ○ The purpose for which facial recognition is being used; and,
	  ○ Where individuals can get additional information about the facial recognition service.
	• Obtain consent from individuals before enrolling an image or facial recognition template in a facial recognition service.
	• *Exception to the consent requirement*: Images or a facial template may be used for a security or safety purpose without obtaining consent subject to the following restrictions:
	  ○ There must be reasonable suspicion;
	  ○ Images or facial templates can only be used for security or safety purposes;
	  ○ Images and facial templates must be maintained in a separate database;
	  ○ The database must be periodically reviewed and facial templates removed that are more than three years or where there is no longer reasonable suspicion; and,
	  ○ Individuals must be allowed to correct or challenge inclusion in the database.
	• Provide meaningful human review for consequential decisions having legal or significant effects on individuals – like denial of finance, lending housing insurance, education, employment or health care, or criminal justice.
	• Test in operational conditions to ensure the best quality results.
	• Train employees operating or using the facial recognition service.

	• Only disclose to law enforcement with consent, a court order, or in emergency circumstances.
Individual Rights **14-4205**	Provides rights for individuals on the use of facial recognition systems: • To know if their image is in a facial recognition system. • To correct and challenge the inclusion of their image for security or safety purposes. • To delete their image. • To withdraw consent for the use of their image. Companies must inform individuals about any actions taken when the individual exercises their rights within 30 days.
Limitations and Applicability **14-4206**	Provides that the act does not restrict entities subject to the act from complying with existing laws.
Enforcement **14-4207**	Provides for Attorney General enforcement and imposition of civil penalties for violations.
	State Government Article **Provides rules on the government's use of facial recognition services.**

Accountability Report by Agencies &
Annual Reporting on the Accountability Report
10-1701
10-1702
10-1703
10-1704
	Agencies using or intending to develop or procure facial recognition services are required to publish a report three months prior to operational use. The report must include:
	• Vendor's name
	• Capabilities and limitations of the service
	• Data that will be used and how it is generated, collected and processed
	• Purpose of proposed use
	• Intended benefits
	• Decisions that will be made based on the service
	• Data management policy, including –
	  ○ How and when the service will be used
	  ○ When and where it will be operated
	  ○ Measures to minimize inadvertent collection of data
	  ○ Integrity and retention policies
	  ○ Rules governing the use of the service
	  ○ Security measures
	  ○ Training procedures
	• Testing procedures, including the process for operational testing
	• Potential impacts on civil rights and liberties, privacy and marginalized communities, and steps to mitigate negative impacts
	• Procedures for receiving and responding to feedback from communities and affected individuals
	
	Prior to finalizing the report consider issues raised during the public review and comment period and community meetings
	
	Update the report every two years

	In addition to the Accountability Report, agencies must publish Annual Reports disclosing: • The extent of the use of facial recognition services

	• A compliance assessment with the terms of the accountability report • Any known or suspected violations of the report or complaints
Meaningful Human Review 10-1705	If used to make decisions having legal or significant effects on individuals there must be meaningful human review of the decision.
Operational Testing 10-1706	Prior to using the facial recognition service agencies must test the service in operational conditions, take steps to ensure best-quality results when the service is being used, and mitigate any material unfair performance differences across subpopulations.
Training of Personnel 10-1707	Agencies must conduct periodic training of employees operating facial recognition services.
Ongoing Surveillance 10-1708	Prohibits ongoing surveillance unless in support of law enforcement activities, may provide evidence of a serious criminal offense, and: • There is a search warrant • Threat of imminent danger, risk of death or serious injury Prohibition on use based on religious, political, or social views or activities or participation in lawful events and organizations, race, ethnicity, citizenship, gender or sexual orientation, or other characteristic protected by law.
Due Process Protections and Record-Keeping 10-1709	Requires agencies to disclose use of a facial recognition service to criminal defendants and requiring maintenance of records for public reporting and auditing. Requires the judiciary to provide information about the number and types of warrants applied for.
Section 2	Specifies that the act is preemptive.
Section 3	This Act shall take effect October 1, 2020