WINSTON
& STRAWN
LLP

BLOG

U.S. Congress Moves to Regulate Facial Recognition Technology

MARCH 18, 2019

The proposed Commercial Facial Recognition Privacy Act of 2019 (the Act), has been introduced in the U.S. Senate to regulate commercial applications of facial recognition technology. The Act applies to private entities that collect, store, or process facial recognition data and regulates how and when they may use "facial recognition technology."

The Act differentiates between processors and controllers—mirroring the language and meaning used in the EU's General Data Protection Regulation (GDPR). The Act prohibits controllers (e.g., the entities making decisions regarding how data is processed) from knowingly using facial recognition technology to collect facial recognition data unless the controller obtains affirmative consent from the consumer *and* provides the consumer with proper notice.

The Act prohibits covered entities from using facial recognition technology to discriminate against consumers, repurposing facial recognition data for a purpose that is different from those disclosed to the consumer, sharing the data with an unaffiliated third party without affirmative consent that is *separate* from the affirmative consent required for initial collection of facial recognition data, and conditioning service on consent by a consumer when the use of facial recognition technology is not necessary for that service.

The Act also seeks to reduce possible bias in facial recognition technology, requiring covered entities to engage in meaningful human review before making any final decision based on the output of facial recognition technology that may result in foreseeable, material "harm" to a consumer or may be unexpected or "highly offensive" to a consumer. Relatedly, if an entity makes a facial recognition technology available as an online service, that entity must allow an independent third party to conduct tests of the technology for accuracy and bias.

The Act contains two exceptions: for either "security applications" or a list of delineated acceptable uses. Federal, state, and local governments are exempt, along with law enforcement, national security, and intelligence agencies. There is no private right of action under the Act. Instead, violations of the Act may be enforced by the FTC or the States' Attorneys General.

The Act expressly states that it does not preempt or affect any current state statute or regulations, except to the extent that the state statute or regulation is inconsistent with the Act. It does not appear that the Act will preempt stricter state laws that regulate facial recognition technology, which include the laws in Illinois, Texas, and Washington (Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/1), Tex. Bus. & Com. § 503.001, and Wash.

Rev. Code § 19.375.010)). In addition to the existing state, proposed state laws are pending in Massachusetts, New York, Delaware, Alaska, Michigan, and Washington. These proposed laws seek to regulate the collection of biometric information, which for many includes the collection of face images and faceprints. While some state legislation is substantially consistent with the Act, others go beyond the Act to impose stricter requirements on par with BIPA.

Learn more about this development in our Global Privacy & Data Security Task Force briefing.

TIP: Companies that use facial recognition technology should understand their notice and consent practices around the facial recognition data and carefully monitor the developing federal and state law.

2 Min Read

Author

Alessandra Swanson

Related Locations

Chicago

Houston

Related Topics

Consumer Privacy

Biometrics

Related Capabilities

Privacy & Data Security

Privacy: Regulated Personal Information (RPI)

Related Regions

North America

Related Professionals

Alessandra Swanson

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.