Commercial Facial Recognition Privacy Act of 2019

Introduced by Senators Roy Blunt (R-MO) and Brian Schatz (D-HI)

The *Commercial Facial Recognition Privacy Act of 2019 (CFRPA)* prohibits commercial entities from using facial recognition (FR) technology to identify or track consumers without obtaining their affirmative consent. Specifically, this bill requires companies to obtain consent before collecting facial recognition data, and present notice when FR is being used. It creates clear definitions and requirements for data controllers and data processors. The bill also addresses accuracy and bias concerns by requiring human review prior to final decisions in cases that may result in harm and online FR providers make an application programming interface available for third-party testing. FR providers are also required to meet data security, minimization, and retention standards as determined by the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST).

Section 1. Short Title

"Commercial Facial Recognition Privacy Act of 2019."

Section 2. Definitions

Selected definitions

- Covered entities: any person, including corporate affiliates, that collects, stores, or processes facial recognition data. Does not include the Federal Government or any State or local government; a law enforcement agency; a national security agency; or an intelligence agency.
- Controller: a covered entity that determines the purposes and means of the processing of facial recognition data.
- Processor: a covered entity that processes facial recognition data on behalf of a controller.
- Facial recognition technology: technology that analyzes facial features in still or video images, and is used to either assign a unique, persistent identifier or for the unique personal identification of a specific individual.
- Security application: loss prevention and any other application intended to detect or prevent criminal activity, including shoplifting and fraud.

Section 3. Prohibited Conduct

- Requires controllers to get affirmative consent from end users before using FR and, after getting consent, provide to end users a notice that FR is present and information on how to access additional documentation when appropriate.
    - When getting consent, controllers must inform end users of the purposes for which the FR will be used, data retention and storage policies, and the process for reviewing, correcting, and deleting FR data.
    - Processors must provide this information to controllers.
- Prohibits the use of FR to discriminate against an end user in violation of applicable Federal or State laws.
- Prohibits repurposing acquired facial recognition data for uses other than the original intent and sharing with unaffiliated third parties without separate consent.
- Prohibits conditioning consent for service, if the use of FR is not necessary for a service.
- Requires meaningful human review prior to making any final decision that may result in reasonably foreseeable harm or may be unexpected or highly offensive.

- For FR that is provided as an online service, requires that the service be available for third-party testing for accuracy and bias through an application programming interface.
- Exempts the following applications from the initial consent and notice requirement:
    - Applications designed for personal file management, or photo or video sorting, or storage, when FR is not used for unique personal identification of a specific individual;
    - Applications used to identify public figures in journalistic media or in copyrighted media for theatrical release;
    - Applications used for an emergency involving imminent danger or risk of death or serious physical injury to an individual.
- Exempts security applications from the consent requirement.
- Allows controllers to scan faces of end users who may not have given consent to verify whether the end user has given consent as long as the controller destroys the data if the end user is not verified.
    - Clarifies that this does not authorize mass scanning of faces in spaces where end users do not have a reasonable expectation that FR is being used on them.

Section 4. Enforcement

- Treats a violation of Section 3 as a violation of a rule defining an unfair or deceptive act or practice under the FTC Act.
- Allows enforcement by State Attorneys General and requires that that State Attorneys General notify the FTC before bringing on a civil action.
    - Allows the FTC to intervene and take over in any State civil action.

Section 5. Regulations

- Gives APA rulemaking authority to the FTC for:
    - Describing data security, minimization, and retention standards for processors, in consultation with the National Institute of Standards and Technology;
    - Defining what is harmful and highly offensive under the human review requirement;
    - Expanding the list of exemptions for the consent and notice requirement.

Section 6. Relation to State Laws

- Does not preempt states from passing stronger laws

Section 7. Relation to Other Privacy and Security Laws

- Declares this Act shall not be used to modify, limit, or supersede any other privacy or security provision in any other Federal or State law.
- Declares this Act shall not be used to limit the authority of the Commission under any other provision of law.

Section 8. Effective Date

- Establishes effective date for the Act as 180 days after the date of enactment.