SENATE, No. 116

STATE OF NEW JERSEY

219th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2020 SESSION

Sponsored by:
Senator NIA H. GILL
District 34 (Essex and Passaic)

SYNOPSIS

Restricts use of facial recognition technology and other biometric recognition by governmental entities.

CURRENT VERSION OF TEXT

Introduced Pending Technical Review by Legislative Counsel.

AN ACT concerning facial recognition and other biometric surveillance and supplementing Title 52 of the Revised Statutes.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. The Legislature finds and declares that:

a. Government use of facial recognition technology poses unique and significant threats to the civil rights and civil liberties of the residents of this State;

b. Facial recognition technology historically has been less accurate in identifying the faces of women, young people, and dark skinned people and these inaccuracies lead to harmful “false positive” identifications;

c. Many of the databases to which facial recognition technology is applied are plagued by racial disparities and other biases, which generate copycat biases in facial recognition data;

d. The broad application of facial recognition technology in public spaces is the functional equivalent of requiring every person to carry and display a personal photo identification card at all times, which constitutes an unacceptable mass violation of privacy;

e. The deployment of other biometric surveillance systems, including gait and voice recognition, raise similar concerns as facial recognition technology;

f. The public use of biometric surveillance systems can chill the exercise of constitutionally protected free speech and association; and

g. The few and speculative benefits of using biometric surveillance systems are greatly outweighed by their substantial harms.

2. As used in this act:

“Biometric surveillance system” means any computer software that performs facial recognition or other remote biometric recognition.

“Facial recognition” means an automated or semi-automated process that assists in identifying a person or capturing information about a person based on the physical characteristics of the person’s face, or that logs characteristics of a person’s face, head, or body to infer emotion, associations, activities, or location of the person.

"Governmental entity" means the State, county, or municipality, or any political subdivision, department, authority, board, bureau, commission, or agency thereof.

“Governmental official” means any officer, employee, agent, contractor, or subcontractor of a governmental entity.

“Other remote biometric recognition” means an automated or semi-automated process that assists in identifying a person or capturing information about a person based on the characteristics of

a person’s gait, voice, or other immutable characteristic ascertained from a distance, or that logs these characteristics to infer emotion, associations, activities, or location of the person, but excludes remote biometric recognition based on DNA, fingerprints, or palm prints.

3. a. Except as provided in subsection b. of this section, the State, any governmental entity of this State, or any governmental official of this State shall not acquire, possess, access, or use any biometric surveillance system, or acquire, possess, access, or use information derived from a biometric surveillance system operated by another entity.

b. A biometric surveillance system, or information derived from the system, may only be acquired, possessed, accessed, or used by the State, any governmental entity of this State, or any governmental official of this State if:

(1) the entities permitted to use the biometric surveillance system, the purposes for this use, and prohibited uses are identified with specificity;

(2) standards are promulgated for the use and management of information derived from the biometric surveillance system, including but not limited to data retention, sharing, access, and audit trails;

(3) auditing practices are developed to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age;

(4) rigorous protections are instituted for due process, privacy, free speech and association, and racial, gender, and religious equity; and

(5) mechanisms to ensure compliance are established.

c. Biometric information obtained in violation of this section shall not be admissible in any criminal, civil, administrative, or other proceeding, except in a judicial proceeding alleging a violation of this section.

d. A person may institute proceedings for a violation of this section for injunctive or declaratory relief in any court of competent jurisdiction to enforce this section, and the person shall be entitled to recover actual damages and additional damages of $100 for each violation, or $1,000, whichever is greater. The court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought pursuant to this subsection.

e. A violation of this section by a State governmental official shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements.

4. This act shall take effect on the first day of the fourth month next following enactment.

STATEMENT

This bill restricts the use of facial technology recognition and other remote biometric recognition by governmental entities and officials of this State.

The bill specifically prohibits acquisitioning, possessing, accessing or using a biometric surveillance system, or the information derived from a biometric surveillance system, operated by another entity unless certain conditions are met. A biometric surveillance system is any computer software that performs facial recognition or other remote biometric recognition. The conditions to be met include: specifically identifying those entities permitted to use the biometric surveillance system and for what purpose; promulgating standards for the use and management of the information, including data retention, sharing, access, and audit trails; developing auditing practices to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age; instituting rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity; and establishing mechanisms to ensure compliance.

Biometric information obtained in violation of the bill's provision is not to be admissible in a criminal, civil, administrative or other proceeding, except in a judicial proceeding alleging a violation of the bill.

The bill authorizes a person to institute proceedings for injunctive or declaratory relief for a violation of the bill's provisions. A person is entitled to recover actual damages, as well as additional damages of $100 for each violation, or $1,000, whichever is greater. Costs and reasonable attorneys' fees are to be awarded to a prevailing plaintiff. A governmental official who violates these provisions may be retrained, suspended, or terminated.