Explanation: Capitals indicate matter added to existing law.
[Brackets] indicate matter deleted from existing law.

*** Warning:** This is an unofficial, introductory copy of the bill.
The official copy considered by the City Council is the first reader copy.

Introductory*

City of Baltimore
Council Bill

Introduced by: Councilmember Burnett

A Bill Entitled

An Ordinance concerning
Facial Recognition Technology
For the purpose of regulating the use of facial recognition technology; requiring possessors of data recovered from facial recognition technology to develop a certain policy regarding retention and destruction of data; establishing certain penalties; defining certain terms; and generally relating to the use of facial recognition technology.

By adding
Article 19 - Police Ordinances
Sections 18-1 to 18-25, to be under the new subtitle designation
"Subtitle 18. Facial Recognition Technology"
Baltimore City Code
(Edition 2000)

Section 1. Be it ordained by the Mayor and City Council of Baltimore, That the Laws of Baltimore City read as follows:

Baltimore City Code

Article 19. Police Ordinances

Subtitle 18. Facial Recognition Technology

Part 1. Definitions; General Provisions.

§ 18-1. Definitions.

(a) *In general.*

In this subtitle, the following words have the meanings indicated.

(b) *Confidential and sensitive information.*

"Confidential and sensitive information" means information that can be used to uniquely identify an individual or an individual's account or property, including:

(1) a genetic marker;

(2) genetic testing information;

(3) a unique identifier number to locate an account or property;

(4) an account number;

(5) a personal identification number;

(6) a passcode;

(7) a driver's license number;

(8) a social security number;

(9) personally identifiable information; and

(10) protected health information.

(c) *Consent.*

"Consent" means a specific, discrete, freely given, unambiguous, and informed agreement given by an individual who is not under any duress or undue influence from a private entity or third party to collect, use, disclose, redisclose, or otherwise disseminate the individual's facial recognition data.

(d) *Department.*

"Department" means the Baltimore Police Department.

(e) *Facial recognition.*

"Facial recognition" means an automated or semi-automated process that assists in identifying or verifying an individual based on the physical characteristics of the individual's face.

(f) *Facial recognition data.*

"Facial recognition data" means information about an individual that is collected, generated, or analyzed by face recognition technology, including:

(1) a single image;

(2) a video sequence;
(3) a view constructed from multiple cameras;

(4) 3 dimensional data used to identify an individual; and

(5) information gathered from the system's analysis of images.

(g) *Facial recognition search.*

"Facial recognition search" means a computer search of facial recognition data to attempt to identify an unidentified person by comparing an image containing the face of the unidentified person to a set of images of identified persons.

(h) *Facial recognition technology.*

"Facial recognition technology" means technology that:

(1) analyzes facial features in still or video images;

(2) is used to assign a unique, persistent identifier; or

(3) is used for the unique personal identification of a specific individual.

(i) *Processor.*

"Processor" means a person who processes, stores, or otherwise uses facial recognition data on behalf of another person.

(j) *Sell.*

(1) *In general.*

"Sell" means the provision of facial recognition data by a private entity to another person for monetary consideration.

(2) *Exclusions.*

"Sell" does not include the provision of facial recognition data:

(i) to a processor on behalf of the private entity; or

(ii) to a 3rd party for the purpose of providing a service or product requested by a consumer.

§§ 18-2 to 18-5. *{Reserved}*

Part 2. Use by City Agencies and Private Entities

§ 18-6. Retention of facial recognition data.

(a) *In general.*

Each person in possession of facial recognition data shall permanently destroy any facial recognition data within 3 years of the date the data was obtained or collected.

(b) *Exceptions.*

Notwithstanding subsection (a) of this section, each person in possession of facial recognition data shall

permanently destroy any data upon the earlier of:

(1) the date on which the initial purpose for collecting or obtaining the facial recognition data has been satisfied; or

(2) within 30 days after receiving a signed request to destroy the facial recognition data submitted by the subject individual or the subject individual's personal representative.

(c) *Security of data.*

Each person in possession of facial recognition data shall store, transmit, and protect from disclosure all facial recognition data:

(1) using a reasonable standard of care; and

(2) in a manner that is as protective as or more protective than the manner in which the person stores, transmits, and protects other confidential and sensitive information.

§ 18-7. Distribution of data.

(a) *In general.*

A person who collects facial recognition data may not sell, lease, or trade an individual's facial recognition data.

(b) *Adverse conditions prohibited.*

(1) A person may not condition the provision of a service on the collection, use, disclosure, transfer, sale, or processing of facial recognition data unless facial recognition data is strictly necessary to provide the service.

(2) A person may not charge different prices or rates for goods or services or provide a different level or quality of a good or service to an individual who exercises the individual's rights under this subtitle.

(c) *Processor may not distribute.*

(1) A person who contracts with a processor to process or store facial recognition data may not allow the processor to collect, store, process, use, disclose, or take any action for monetary consideration on or with the facial recognition data of an individual, except for the purpose for which the person received consent from the individual.

(2) Except as authorized by a contract with a person who legally possesses the facial recognition data, a processor may not collect, store, process, use, disclose, or take any action for monetary consideration on or with the facial recognition data.

§ 18-8. Consent for distribution.

(a) *In general.*

Except as provided in subsection (b) of this section, a person who collects facial recognition data may not collect, use, disclose, redisclose, or otherwise disseminate an individual's facial recognition data unless:

(1) the individual or the individual's legally authorized representative gives consent to the collection, use, disclosure, redisclosure, or dissemination; or

(2) the disclosure or redisclosure is required:

(i) by a valid warrant or subpoena;

(ii) to comply with federal, State, or local laws, rules, or regulations; or

(iii) to cooperate with law enforcement concerning conduct or activity that the private entity or the processor reasonably and in good faith believes violates a federal, State, or local law, rule, or regulation.

(b) *Exceptions.*

A person may collect, use, disclose, redisclose, or otherwise disseminate an individual's facial recognition data without complying with subsection (a) of this section if the person:

(1) collects, uses, discloses, rediscloses, or otherwise disseminates the facial recognition data for fraud prevention or the protection of an individual's confidential and sensitive data; and

(2) subject to subsection (c) of this section, posts conspicuous written notice of the collection of facial recognition data at each point of entry of the area in which collection of facial recognition data will occur.

(c) *Form of consent.*

An individual may give consent for the collection, use, disclosure, redisclosure, or dissemination of the individual's facial recognition data through the following means:

(1) a written statement;

(2) a written statement by electronic means; or

(3) in the context of employment, a release executed by an employee as a condition of employment.

(d) *Contents of notice.*

The notice required in subsection (b)(2) of this section shall inform an individual of:

(1) the categories of facial recognition data to be collected;

(2) the purposes for which the categories of facial recognition data will be used; and

(3) the length of time the facial recognition data will be retained.

(e) *Use tied to services.*

The collection, use, disclosure, redisclosure, or other dissemination of facial recognition data under this subsection shall be directly tied to the services being provided to the individual.

§ 18-9. Required disclosure.

(a) *In general.*

A person who collects, uses, discloses, or rediscloses facial recognition data of an individual must, at the request of the individual or the individual's legally authorized agent, disclose, free of charge, the facial recognition data and information related to the use of the facial recognition data to the individual, including:

(1) the categories of facial recognition data; and

(2) the purposes for which the person used the facial recognition data.

(b) *Limits on disclosure.*

A person may not be required to disclose the information described in subsection (a) of this section to an individual or the individual's legally authorized representative more than twice during any consecutive 12-month period.

§§ 18-10 to 18-15. ***{Reserved}***

Part 3. Use by Baltimore Police Department

§ 18-16. Use by police.

This subtitle shall apply to the Baltimore Police Department.

§ 18-17. Required evaluation of technology.

(a) *Technology standards.*

All technology used by the Department to conduct a facial recognition search must:

(1) be evaluated by the National Institute of Standards and Technology;

(2) in the Face Recognition Vendor Test, must:

(i) receive an accuracy score of 98% or higher for true positives across all demographic groups; and

(ii) display minimal performance variations across demographics associated with:

(A) race;

(B) skin tone;

(C) ethnicity; and

(D) gender.

(b) *Vendor requirements.*

The Department must obtain all technology used to conduct a facial recognition search from a vendor that provides annual independent assessments and benchmarks from the National Institute of Standards and Technology.

§ 18-18. Use of generated image.

(a) *Prohibition.*

The Department may not use the match of an image generated using a facial recognition search in an affidavit to constitute probable cause for the issuance of either:

(1) a search warrant; or

(2) an arrest warrant.

(b) *Exculpatory evidence.*

The Department may use the match of an image generated using a facial recognition search as exculpatory evidence.

§ 18-19. Use at protests, rallies, etc.

The Department may not conduct facial recognition searches at:

(1) a protest;

(2) a rally; or

(3) another gathering that is protected by the 1st Amendment to the United States Constitution.

§ 18-20. Documentation of search.

(a) *In general.*

The Department shall keep record of:

(1) each facial recognition search performed by the Department;

(2) each request made to the Department by a law enforcement agency or federal agency for a facial recognition search; and

(3) each request made by the Department to the Federal Bureau of Investigation for a facial recognition search.

(b) *Contents of record.*

The documentation described in subsection (a) of this section shall include:

(1) the date and time of the search or request;

(2) the race and gender of the subject of the search or request;

(3) the number of matches returned, if any;

(4) the name and position of the requesting individual and employing law enforcement agency;

(5) a copy of the warrant, or in the case of an emergency, a copy of the written emergency request;

and

(6) data detailing any individual characteristics included in the facial recognition search or request.

(c) *Public access to record.*

The records described under this subsection shall be made publicly available.

§ 18-21. Required notice.

(a) *In general.*

An individual identified by facial recognition technology under this part shall be provided notice that the individual was subject to a search within 7 days after the Department receives records or other information resulting from the search.

(b) *Delayed notice.*

The Department may apply for a court order to extend the time period between the facial recognition search and the notification required under subsection (a) of this section.

(c) *Issuance of delayed notice.*

The order described in subsection (b) of this section shall be issued by:

(1) the court that issued the order authorizing the facial recognition search; or

(2) in the case of an emergency search, the court where the sworn statement setting forth the grounds for the emergency search was filed.

(d) *Contents of order for delayed notice.*

The order for delayed notice described in subsection (b) of this section shall detail, to the fullest extent possible without endangering the public, the reasons why providing notice to the individual subjected to the facial recognition search would constitute an immediate threat to public safety.

(e) *Duration of order for delayed notice.*

The order described in subsection (b) of this section may not be valid for more than 7 days without an additional order for delayed notice.

§ 18-22. Annual report.

(a) *In general.*

No later than March 31 of each year, the Department shall publish on its website the following data for the previous calendar year:

(1) the total number of facial recognition searches performed by the Department, dis-aggregated by the law enforcement agency or federal agency on whose behalf the search was performed; and

(2) the total number of facial recognition searches performed by the Federal Bureau of Investigation on behalf of the Department.

powered by Legistar™

(b) *Required information.*

For each category of data and each law enforcement agency included in the report, the published information shall include:

(1) the number of searches performed pursuant to a warrant;

(2) the alleged offense being investigated;

(3) the number of searches performed pursuant to an emergency; and

(4) the race and gender of the subject of the search.

§ 18-23. Required retention of information.

In addition to the reporting requirements established under this subtitle, the Department must collect and retain the following information for future disclosure during the course of criminal proceedings and post-conviction proceedings:

(1) a complete history of the search queries made by each individual that conducts a facial recognitions search;

(2) the total number of searches conducted using the face recognition technology;

(3) the number of searches that resulted in the facial recognition technology offering individuals matching the characteristics of the individual in the image used to conduct the search;

(4) the number of times that the use of the facial recognition technology offered an investigative lead;

(5) the number of cases closed by arrest where an investigative lead offered by facial recognition technology was a contributing factor;

(6) the suspected criminal offense being investigated for each search conducted;

(7) the image repository being compared or queried to conduct a facial recognition search;

(8) demographic information on individuals whose images were searched; and

(9) records detailing any other entities that received facial recognition data shared by the Department.

§ 18-24. Oversight and enforcement.

(a) *In general.*

Any person who is subject to a violation of this subtitle or is harmed by improper use of recognition technology by the Baltimore Police Department may file for injunctive relief in a court of competent jurisdiction.

(b) *Violation by City employee.*

Any violation of this subtitle by an employee of the Department shall, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining

powered by Legistar™

units, result in consequences that may include:

(1) training requirements;

(2) suspension from employment; and

(3) termination of employment.

(c) *Disclosure of recognition technology use.*

To the extent permitted by law, the Department shall publicly disclose all of its recognition technology-related contracts, including any and all non-disclosure agreements.

§ 18-25. Whistleblower protection.

(a) *In general.*

Neither the Department nor any person acting as an agent on behalf of the Department may take or threaten to take a personnel action with respect to any employee or applicant for employment because:

(1) the employee or applicant for employment was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a recognition technology or recognition data, if the employee or applicant had a good faith belief that the disclosure evidenced a violation of the subtitle; or

(2) the employee or applicant was perceived to, about to, assisted, or participated in any proceeding or action to carry out the purposes of this subtitle.

(b) *Disciplinary action.*

An employee or any person acting on behalf of the Department shall be subject to disciplinary action for violating the provisions of subsection (a) of this section.

(c) *Relief.*

Any employee or applicant who is injured by a violation of this subsection may file for injunctive relief in any court of competent jurisdiction.

Section 2. And be it further ordained, That the enforceability of Part 3 {"Use by Baltimore Police Department"} of this Ordinance is contingent upon State action amending City Charter Article II, § 27 to strike certain language that prohibits any ordinance of the City or act of any municipal officer from conflicting, impeding, obstructing, hindering, or interfering with the powers of the Police Commissioner.

Section 3. And be it further ordained, That this Ordinance takes effect on the 90th day after the date it is enacted.