USE OF FACIAL RECOGNITION TECHNOLOGY

FC No.: 0627
Date: 03-07-2022

If a provision of a regulation, departmental directive, or rule conflict with a provision of the contract, the contract prevails except where the contract provision conflicts with State law or the Police Collective Bargaining Law. (FOP Contract, Article 61)

Contents:

I. Purpose

The purpose of this policy is to provide guidance on the Montgomery County Department of Police's (MCPD) use of facial recognition technology to establish procedures for its proper use and accountability. Facial recognition technology involves a computer system's automated search of a human face using biometric algorithms to identify similar facial images within a database (one-to-many). This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. MCPD uses facial recognition technologies to support the investigative efforts of law enforcement and public safety agencies both within and outside of Montgomery County, Maryland.

II. Policy

The policy of MCPD is to utilize facial recognition technology in a manner that is consistent with authorized purposes to protect the community as well as civil rights and civil liberties. Candidate images provided by facial recognition technology will be evaluated by a qualified investigator (Section IV. Paragraph D). An identified candidate(s) provided by the qualified investigator is an investigative lead and <u>cannot</u> be considered a positive identification without further investigation.

III. Definitions

A. <u>Biometric</u>: A general term used alternatively to describe automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

B. <u>Biometric Template</u>: A set of biometric measurement data (or features) prepared by a facial recognition system from a face image.

C. <u>Candidate Images</u>: A list of most likely images that were determined by the software to be sufficiently similar to the probe image to warrant further analysis.

D. Database: A location where a group of images of known individuals and biometric templates are stored and managed. An image database is searched during a facial recognition search process whereby a probe image is used by facial recognition software for comparison with the images (or features within images) contained in the image database.

E. Facial Recognition: A form of artificial intelligence (AI) that is applied to conduct an automated search of a facial image. The facial image is searched within a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity.

F. Facial Identification: The human element of the manual comparison of faces. The manual examination of the differences and similarities between two facial images or a live subject and a facial image (one-to-one) for the purpose of determining if they represent the same person.

G. Probe Image: The image submitted for searching and comparison against images contained in a facial recognition database.

IV. Procedures

A. Approved Uses of Facial Recognition Technology
The use of facial recognition technology may only be used by trained personnel designated by the Director, SID, or designee for the following circumstances:

1. To assist in the investigation of the following enumerated crimes:
   a. A crime of violence as defined in Section 14-101(a) of the Criminal Law Article of the Maryland Code.
   b. Crimes related to firearm possession.
   c. Incidents related to investigations for an Extreme Risk Protection Order.
   d. Crimes related to Child Abuse.
   e. Crimes related to Child Pornography.
   f. Crimes related to Domestic Violence.
   g. Crimes related to Terrorism.
   h. Crimes related to Human Trafficking
2. To locate subjects for the service of ex-parte orders, arrest warrants, and search warrants of the above enumerated crimes (Section IV. A. 1.)
3. To assist in the identification of potential witnesses and/or victims of the above enumerated crimes (Section IV. A. 1).
4. To mitigate an imminent threat to health or safety
5. To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (i.e. incapacitated, deceased, or otherwise at-risk individual).
6. To support law enforcement in critical incident responses.
7. To assist with other official law enforcement purposes with the approval of the Director, Special Investigations Division, or designee after considering the following factors:
   a. Crime trends;
   b. Criminal severity of an offense
   c. Relation organized crime;
   d. Relation to hate/bias incident
   e. Community impact
   f. Cruelty to animals;
   g. Risk to the community
   h. The potential to negate an individual's involvement in an investigation; or
   i. The potential infringement or perceived infringement on privacy rights.

B. Prohibited Uses of Facial Recognition Technology

1. MCPD respects the First Amendment Rights of individuals and will not utilize facial recognition technology for individuals based solely on the following:
    a. Religious, political, or social views or activities;
    b. Participation in a noncriminal organization or lawful event;
    c. Race, ethnicity, citizenship, places of origin, age, disability, gender, gender identity, sexual orientation, or any other classification protected by law.
2. MCPD personnel are prohibited from using facial recognition technology to assess immigration status or assist in the enforcement of immigration law.
3. A candidate image generated by facial recognition technology and reviewed for facial identification is an investigative lead ONLY and DOES NOT establish probable cause to obtain an arrest warrant without further investigation.

C. Facial Recognition Searches

1. Facial recognition searches may only be performed by Department personnel who have been trained in the use of facial recognition software and facial comparison and identification as approved by the Director, SID, or designee.
2. MCPD personnel designated to utilize facial recognition technology will attend bias training in accordance with state law.
3. Self-initiated facial recognition searches on crime alert bulletins from other agencies may be conducted by department personnel trained and approved in the use of facial recognition.
4. Facial recognition technology use must comply with departmental policy.
5. Facial recognition technology may not be knowingly used to assist law enforcement agencies in a manner that contradicts their policy or legislation unless information obtained prior to that knowledge is determined to be critical to the immediate preservation of life.

D. Process for Requesting Facial Recognition Technology Assistance

MCPD requests for facial recognition technology assistance shall be electronically submitted to the Digital Intelligence Analysis Unit (DIAU), SID through the DIAU Help Desk System. If a DIAU Help Desk System request is not possible, MCPD or outside law enforcement agencies shall be directed to submit a written request to include the requester's contact information, reference/incident/case number, type of investigation, and justification for utilization of facial recognition technology.

E. Facial Recognition Technology Results

All MCPD results obtained by facial recognition technology will be provided to the requester in writing and contain the following information:

1. Facial recognition technology was utilized to develop the provided investigative lead;
2. Information contained within the investigative lead is not a positive identification of any individual; and
3. Investigative leads do not establish probable cause and require further investigation

V. Maintenance of Records

A. The use of facial recognition technology will be audited by the Office of the Chief, Professional Accountability Division. The requester will be required to provide appropriate justification for the request of facial recognition technology assistance.

B. Appropriate justification will include the requester's contact information, reference number, and justification for utilization of facial recognition technology.

C. The Office of the Chief, Professional Accountability Division will implement the audit procedures ***and*** conduct reviews of necessary records.

D. The department shall track, when applicable, the perceived race of any suspects juxtaposed with the race of any investigative leads developed with the program.

VI. CALEA Standards: ***1.2.3, 1.2.5, 1.2.9, 26.1.1, 41.2.5, 41.2.6, 41.2.7, 42.2.1, 43.1.1, 46.1.2, 46.1.3, 46.1.4, 46.1.5, 46.1.6, 82.2.1, 82.2.2, 83.2.1, 83.3.2***

VII. Proponent Unit: Special Investigations Division

VIII. Cancellation: None

Marcus G. Jones
Chief of Police