MONTGOMERY COUNTY MARYLAND
DEPARTMENT OF POLICE

USE OF FACIAL RECOGNITION TECHNOLOGY

DIRECTIVE NO: **FC 0627**	**EFFECTIVE DATE:** **October 1, 2024**
REPLACES: FC 0627, dated March 7, 2022	**ACCREDITATION STANDARDS:** CALEA Standards: 6th Edition, 1.2.3, 1.2.5, 26.1.1, 41.2.5, 41.2.6, 41.2.7, 42.2.1, 46.1.2, 46.1.5, 82.2.1
PROPONENT UNIT: Special Investigations Division	**AUTHORITY:** **Marc R. Yamada, Chief of Police**

If a provision of a regulation, departmental directive, rule, or procedure conflicts 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).

I. POLICY

The policy of the Montgomery County Department of Police (MCPD) is to utilize facial recognition technology in a manner consistent with authorized purposes to protect the community, civil rights, and civil liberties. A qualified investigator will evaluate candidate images provided by facial recognition technology (Section IV. Paragraph D). An identified candidate(s) provided by the qualified investigator is an investigative lead and cannot be considered a positive identification without further investigation. **The department will comply with all requirements of Maryland Criminal Procedure §2-501 et seq. "Facial Recognition Technology."**

This policy does not regulate the agencies' ability to utilize facial features to grant or deny access to electronic devices, facilities, or other non-investigatory purposes. Nor does it regulate the agency's ability to utilize automated or semi-automated processes for redacting images or recordings for release.

The Director of the Special Investigations Division (SID) oversees and administers Facial Recognition Technology in compliance with Maryland Law and local laws, regulations, and policies.

II. PURPOSE

The purpose of this policy is to provide guidance on MCPD's 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 identify 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.

III. DEFINITIONS

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

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

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

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

E. Facial Recognition: **A computer program, service, or any other technology that analyzes facial features and is used by or at the direction of a law enforcement agency for the verification or persistent tracking of individuals in still or video images for use in criminal investigations**.

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) to determine 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 Criminal Law Article §14-101(a)

b. A human trafficking offense under Criminal Law Article Title 3, subtitle 11,

c. First or Second-Degree Child abuse under Criminal Law Article §3-601,

d. Child Pornography Offense under Criminal Law Article §11-207,

e. A hate crime under Criminal Law Article §10-304,

f. A weapon crime under Criminal Law Article §4-102, §4-103, §4-203(a)(1)(iii) or (iv), §4-204, or §4-303(a)(2),

g. A weapon crime under Public Safety Article §5-138, §5-140, §5-141, §5-207(c)(16), §5-406(a)(3), or §5-703(a),

h. Aggravated Cruelty to Animals under Criminal Law Article §10-606 or §10-607,

i. Importation of Fentanyl or a Fentanyl analog under Criminal Law Article §5-614 (A)(1)(xii),

j. Stalking under Criminal Law Article §3-802.

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). **This includes an investigation to locate a fugitive from justice from another state who is wanted for a crime substantively equivalent to the above-enumerated crimes.**

3. To assist in identifying potential witnesses and/or victims of the above-enumerated crimes (Section IV.A.1).

4. To mitigate **a criminal act involving circumstances presenting a substantial and ongoing threat to public safety or national security.**

5. To assist in identifying a person who lacks capacity or is otherwise unable to identify themselves (i.e., incapacitated, deceased, or otherwise at-risk individual).

B. <u>Prohibited Uses of Facial Recognition Technology</u>

1. MCPD respects the **constitutional rights** of individuals and will not utilize facial recognition technology **on a subject who is engaged in activity protected under the United States Constitution, the Maryland Constitution, or the Maryland Declaration of Rights unless there is reasonable suspicion to believe that the individual has committed, is in the process of committing, or is about to commit a crime listed above**.

2. Facial recognition technology may not be utilized based solely on:

a. **Personal interest not related to legitimate duties or objectives of the law enforcement agency;**

b. **An individual's political or social beliefs;**

c. **An individual's participation in lawful activities or**

d. **An individual's race, color, religious beliefs, sexual orientation, gender, disability, national origin, or status as homeless.**

3. MCPD Personnel are prohibited from using facial recognition technology to assess immigration status or assist in enforcing immigration law.

4. Personnel are prohibited from using facial recognition technology to analyze a sketch or manually produce an image.

5. Personnel may not disclose to a witness in a criminal investigation, prior to the witness participating in a live identification or photo array, that a particular suspect or image of a suspect was identified using facial recognition technology.

6. When creating a photo array, personnel may not utilize as a suspect image the same image that resulted from the use of facial recognition technology.

7. **Facial recognition technology may not be used for the purpose of live or real-time identification of an image or recording.**

C. Facial Recognition Searches

1. MCPD personnel designated by the Director, SID, or designee to utilize facial recognition technology will be trained in face comparison and identification and attend **annual** training in accordance with state law.

   a. **The department shall only utilize databases or systems for Facial Recognition Searches that comply with Maryland Law.**

2. **All facial recognition leads shall be independently verified by an individual authorized to use facial recognition technology.**

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 may not be knowingly used to assist law enforcement agencies in a manner that contradicts their policy or legislation.

D. Process for Requesting Facial Recognition Technology Assistance

MCPD facial recognition technology assistance requests 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, and justification **(i.e., the specific enumerated crime or other permissible authorized use)** 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. **Results generated by facial recognition technology may only be considered or introduced as evidence in connection with a criminal proceeding for the purpose of establishing probable cause or positive identification in connection with the issuance of a warrant or at a preliminary hearing; however, facial recognition results may not be the sole basis to establish probable cause of an individual and require support by additional, independently obtained evidence. Additionally, facial recognition technology results may not be introduced as evidence in a criminal trial or in an adjudicatory hearing held under 3-8A-18 of the Courts Article (juvenile adjudication) in accordance with state law.**

4. **A summary indicating:**

   a. **The name of each facial recognition system used.**

   b. **A description and the name of the databases searched.**

   c. **Any results generated that led to further investigative action from each database or system used.**

V. AUDITS AND MAINTENANCE OF RECORDS

A. The use of facial recognition technology will be audited **annually by October 1st** by the Professional Accountability Division (PAD). **The audit will be to determine compliance with state law and department policy, to include:**

1. **Ensuring discovery reports contain the names of each facial recognition system used, a description, and the names of the databases searched and generated results from the use of the facial recognition technology that led to further investigative action;**

2. **Ensuring SID personnel designated to utilize facial recognition technology have attended the required training in accordance with departmental policy and state law;**

3. **Ensuring that all required annual reports were completed and that required disclosures are posted on the department's website;**

4. **Ensuring that the "Facial Recognition Annual Data (FRAD) Report" referenced in Section VI was published and submitted to the Governor's Office of Crime Prevention and Policy (GOCPP).**

5. **The PAD audit will include the number of searches, the type of crime with each incident, and the total number of possible matches, which include the age, race, and gender of individuals.**

B. **The department shall maintain the audit results for at least three years.**

C. **The audit results and any reference materials shall be disclosed if requested by an entity referenced under Maryland law.**

VI. REPORTING REQUIREMENTS

A. The MCPD's Facial Recognition Technology Administrator or designee is responsible for preparing and publishing a "Facial Recognition Annual Data (FRAD) Report."

1. **If not specified, the SID Director will assume this role.**

2. **The FRAD Report will be published by February 1st of each year.**

3. **The FRAD Report will be sent to the GOCPP by May 1st of each year.**

B. The "Facial Recognition Annual Data (FRAD) Report" will detail the use of facial recognition technology <u>by authorized SID personnel</u> for the previous calendar year and include:

1. **The name of each facial recognition system/database used.**

2. **The number of facial recognition searches used for each system.**

3. **The justification (i.e., the specific enumerated crime or other authorized use) for each search.**

4. **The total number of possible matches that led to further investigative action for each search, including the following:**

   a. **Age**
   b. **Race**
   c. **Gender**

5. **Of the individuals connected to the possible matches returned, if the information is available from the government records searched.**

6. **Any and all data breaches or unauthorized uses of facial recognition technology under the agency's control.**

C. This Function Code is the department's "use and data management policy" on facial recognition technology.

D. The department shall post on its website:

1. **A copy of this policy;**
2. **The names of all nongovernmental facial recognition systems utilized and**
3. **The names and descriptions of all nongovernmental databases searched.**