PATROL GUIDE

Section: Command Operations		Procedure No: 212-129	
FACIAL RECOGNITION TECHNOLOGY			
DATE ISSUED: 03/12/20	DATE EFFECTIVE: 03/12/20	REVISION NUMBER:	PAGE: 1 of 4

PURPOSE

To ensure the use of facial recognition technology balances the need for effective, accurate law enforcement investigations, and the need to respect the privacy of citizens.

SCOPE

Facial recognition technology enhances the ability to investigate criminal activity and increases public safety. The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

DEFINITIONS

AUTHORIZED USES - Facial recognition technology must only be used for legitimate law enforcement purposes. Specifically, the following are the only authorized uses for employing facial recognition technology:

a. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime,
b. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity,
c. To identify a deceased person,
d. To identify a person who is incapacitated or otherwise unable to identify themselves,
e. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else’s identification, or a false identification, or
f. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot, etc.).

PROBE IMAGE - An image of an unidentified person obtained by the assigned investigator from witnesses, victims, or other reliable sources.

PHOTO REPOSITORY - The controlled and limited group of images against which the probe image is compared. The photo repository only contains arrest and parole photographs. It is stored in a designated, and approved, law enforcement database, and access is restricted to authorized users.

BACKGROUND CHECK - A Real Time Crime Center, Facial Identification Section (RTCC-FIS) investigator evaluates the reliability of a potential match between the probe image and an image from the photo repository. This includes an assessment of available information about the potential match, and relevant details of the investigation.

DEFINITIONS (continued)

VISUAL COMPARISON - A RTCC-FIS investigator visually compares the differences and similarities between a probe image and a potential match from the photo repository for the purpose of evaluating whether they represent the same person. In general, during this process, an investigator/supervisor compares facial characteristics (e.g., eyes, ears, nose, chin, mouth, hair, overall facial structure, any scars, marks, blemishes, or tattoos, etc.) and general characteristics, such as overall complexion, gender, and age.

POSSIBLE MATCH CANDIDATE - A potential suspect who is identified through a complete facial recognition analysis, which includes facial recognition technology, visual comparison, background investigation and supervisory review. A possible match candidate shall be treated as an investigative lead only. It does not by itself establish probable cause to make an arrest, or obtain an arrest or search warrant. Corroborating information must be developed through additional investigation by the assigned investigator.

PROCEDURE

When an investigator obtains an image depicting the face of an unidentified suspect, victim or witness, and intends to identify the individual using facial recognition technology, which includes any digital comparison of the probe image to photos stored in the photo repository, the assigned investigator must submit a request to the RTCC-FIS for facial recognition analysis:

FACIAL IDENTIFICATION SECTION PERFORMS FACIAL RECOGNITION ANALYSIS:

ASSIGNED INVESTIGATOR

1. Obtain image(s)/video(s) of individual to be identified.
   a. If video is submitted, include associated software/player.
   b. If image is from internet/social media, include site link.
2. Upload image(s) to Enterprise Case Management System (ECMS) and submit request to Real Time Crime Center-Facial Identification Section (RTCC-FIS) for facial recognition analysis via an **FIS Request DD5**.

NOTE

*Investigators who do not have access to the Enterprise Case Management System (ECMS) may contact RTCC-FIS via phone or email. Investigators must provide a case or **COMPLAINT REPORT (PD313-152)** number. RTCC-FIS will generate an **FIS Request DD5**.*

RTCC-FIS SUPERVISOR

3. Assign FIS number to request upon receipt of **FIS Request DD5** via ECMS, and direct RTCC-FIS investigator to review request.

RTCC-FIS INVESTIGATOR

4. Confirm underlying basis for request is in compliance with authorized uses of facial recognition technology.
   a. Document confirmation in ECMS.
5. Select probe image of individual to be identified from images submitted.
   a. If image quality is unsuitable for facial recognition comparison, notify the assigned investigator via **FIS Image Rejection Report**.
   b. Permit assigned investigator to submit additional images.

RTCC-FIS INVESTIGATOR (continued)

6. Run query using facial recognition technology for comparison of probe image to images stored in photo repository, and generate pool of possible match candidates.

7. Review and analyze results by performing a visual comparison.

8. Perform detailed background check to confirm reliability of match, if possible match candidate is identified.

9. Submit possible match candidate for peer review.

RTCC-FIS SUPERVISOR

10. Conduct final review of possible match candidate, and approve, if appropriate.

11. Direct RTCC-FIS investigator to provide possible match candidate to assigned investigator via **FIS Possible Match Report**, if in agreement with findings.

12. Direct RTCC-FIS investigator to continue investigation for possible match candidate, if not in agreement with findings of RTCC-FIS investigator.

    a. Direct RTCC-FIS investigator to report negative results to assigned investigator via **FIS No Match Report**, if possible match candidate is not identified or approved by supervisor.

RTCC-FIS INVESTIGATOR

13. Prepare **FIS Possible Match Report** and upload to assigned investigator's ECMS case file, if supervisor confirms possible match candidate.

    a. **FIS Possible Match Report** shall include probe image, and notification stating that determination of a possible match candidate alone does not constitute probable cause to effect an arrest, or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

    b. Forward **FIS Possible Match Report** using same method used to submit request for facial recognition analysis, if request is from outside law enforcement agency.

14. Retain all records of facial recognition searches, including associated FIS case number, reason each search was requested, details, and search results, and upload them into the ECMS case file.

ASSIGNED INVESTIGATOR

15. Conduct further investigation to determine whether possible match candidate is connected to, or involved in, incident under investigation, upon receipt of **FIS Possible Match Report** in order to establish probable cause.

16. Continue investigation, (i.e., obtaining additional suitable images for another submission to RTCC-FIS), if no possible match candidate was determined, or image was rejected.

ADDITIONAL DATA

The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited, unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Detectives or Deputy Commissioner, Intelligence and Counterterrorism.

RTCC-FIS and Detective Squad supervisors shall comply with P.G. 219-14, "Department Computer Systems" to evaluate and monitor compliance with this procedure by investigators who utilize facial recognition technology.

ADDITIONAL DATA (continued)

All records related to facial recognition requests and results will be subject to privacy, confidentiality, and dissemination restrictions, as per P.G. 212-76, "Information Concerning Official Business of Department," as well as all related procedures and applicable local and federal laws/rules.

Members of the Detective Bureau should direct all requests from outside agencies to RTCC-FIS on an "FIS Outside Agency Form." A copy of a complaint report from another law enforcement agency must be submitted with the "FIS Outside Agency Form."

The Intelligence Bureau shall also follow an analogous procedure when Intelligence Bureau investigators utilize facial recognition technology and will abide by Handschu Guidelines whenever they apply.

RELATED PROCEDURES

Department Confidentiality Policy (P.G. 203-22)
Information Concerning Official Business of Department (P.G. 212-76)
Department Computer Systems (P.G. 219-14)

FORMS AND REPORTS

COMPLAINT REPORT (PD313-152)
FIS Request DD5
FIS Possible Match Report
FIS No Match Report
FIS Image Rejection Report