PLANNING AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF:  James E. Craig, Chief of Police


SUBJECT:  FACIAL RECOGNITION

ORIGINATED OR REQUESTED BY:  Planning, Research and Deployment

APPROVALS OR COMMENTS:  The above referenced directive is updated to reflect the Board of Police Commissioners and internal review.

APPROVED  JUL 25 2019
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

APPROVED  JUL 25 2019
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

RECEIVED  JUL 25 2019
BOARD OF POLICE COMMISSIONERS

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO
PLANNING AND DEPLOYMENT.
1301 Third Street, 7th Floor, Detroit MI 48226
FACIAL RECOGNITION

307.5 - 1 PURPOSE
The purpose of this policy is to establish acceptable use for the Detroit Police Department's (DPD) facial recognition software.

307.5 - 2 Prohibited Uses
307.5 - 2.1 Surveillance
Members shall not use facial recognition software to surveil the public through any camera or video device.

307.5 - 2.2 Live Streaming or Recorded Videos
Members shall not use facial recognition software on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

307.5 - 2.3 First Amendment Events
The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request facial recognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;
b. Their participation in a particular noncriminal organization or lawful event; or
c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

307.5 - 3 Discipline
Any violations to this policy shall be deemed major misconduct. Any misuse of the facial recognition software will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

307.5 - 4 Use of Facial Recognition Technology
307.5 - 4.1 Use Limited to Still Images
Facial recognition software may only be used on a still image of an individual.
307.5 Facial Recognition

307.5 - 4.2 Criminal Investigation Required
Members shall not use facial recognition technology unless that technology is in support of an active or ongoing Part 1 Violent Crime investigation (e.g. robbery, sexual assault, or homicide) or a Home Invasion 1 investigation.

307.5 - 4.3 Individualized Targeting
Members shall not use facial recognition technology on any person unless there is reasonable suspicion that such use of facial recognition technology will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion 1 investigation.

307.5 - 4.4 Process for Requesting Facial Recognition
1. Requests for facial recognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information.
2. CIU shall perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP) which include criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state’s database. Any such request must be approved by a CIU supervisor.
3. If the examiner detects an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor.
4. Upon final approval, CIU shall complete a supplemental incident report for the requestor. The supplemental incident report shall detail how the examiner came to their conclusion.
5. In the event that a viable candidate cannot be located, the requestor will be notified that no candidate was identified.
6. If CIU cannot discern a viable candidate, the photograph of the suspect will be purged from the facial recognition system.

307.5 - 5 Governance and Oversight
307.5 - 5.1 Report to the Board of Police Commissioners
DPD shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of facial recognition requests that were fulfilled, the crimes that the facial recognition requests were attempting to solve, and the number of leads produced from the facial recognition software.