Series	Effective Date	Review Date	Directive Number
300 Support Services	09/19/2019	Annually	307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			☒ New Directive ☐ Revised
References:			

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. Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation. If a match is found through DPD's Facial Recognition Process, it shall be considered an investigative lead, and the requesting investigator shall continue to conduct a thorough and comprehensive investigation.

307.5 - 2 Definitions

307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.

307.5 - 2.2 DataWorksPlus

The facial recognition software with which the Department has a contract.

307.5 - 2.3 Examiner

An individual who has received advanced training in the facial recognition system and its features. Examiners have at least a working knowledge of the limitations of facial recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for facial recognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.4 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

307.5 - 2.5 Highly Restricted Personal Information
An individual's photograph or image, social security number, digitized signature, medical and disability information.

307.5 - 2.6 Home Invasion I
Unlawful entry of a dwelling with intent to commit or committing a felony, larceny, or assault on the home when either the unlawful entrant is armed with a dangerous weapon or when another person is lawfully present in the dwelling.

307.5 - 2.7 Part 1 Violent Crimes
For the purposes of this directive, Part 1 Violent Crimes are defined as robbery, sexual assault, aggravated assault, or homicide.

307.5 - 2.8 Personally Identifiable Information (PII)
Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

307.5 - 2.9 Reasonable Suspicion
The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

307.5 - 2.10 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

307.5 - 3 Prohibited Uses

307.5 - 3.1 Surveillance
Members shall not use facial recognition to surveil the public through any camera or video device.

307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use facial recognition 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 - 3.3 Mobile Facial Recognition
Members shall not use mobile facial recognition.

307.5 - 3.4 Predictive Analysis
Members shall not use facial recognition for predictive analysis.

307.5 - 3.5 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 - 3.6 Facial Recognition Use for Immigration Enforcement

DPD members are strictly prohibited from using facial recognition to assess immigration status.

307.5 - 4 Discipline

1. 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.
2. If facial recognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

307.5 - 5 Use of Facial Recognition Technology

307.5 - 5.1 Use Limited to Still Images

Facial recognition software may only be used on a still image of an individual.

307.5 - 5.2 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 - 5.3 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 I investigation.

307.5 - 5.4 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. Photographs shall be handled as specified in Manual Directive 306.1 Evidence Property.

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. The corroboration must have written sign-off by the supervisor and all examiners' involved.
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, and include the following language:

   "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."

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 removed from the facial recognition system.

307.5 - 5.5 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request searches to assist with investigations only if the following requirements are met:

a. Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between the Detroit Police Department and the outside agency;
b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

   - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."

c. If any agency is found not in compliance with this Directive, the Department shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

307.5 - 6 Governance and Oversight

307.5 - 6.1 LASO & Crime Intel Responsibilities

1. The primary responsibility for the operation of the Department's criminal justice information systems, facial recognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.
2. The LASO will be responsible for the following:

    a. Overseeing and administering the facial recognition program to ensure compliance with applicable laws, regulations, standards, and policy;
    b. Acting as the authorizing official for individual access to facial recognition information;
    c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
    d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

3. The commanding officer of the Crime Intelligence Unit will be responsible for the following:

    a. Reviewing facial recognition search requests, reviewing the results of facial recognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
    b. Ensuring that protocols are followed to ensure that facial recognition information (including probe images) is automatically purged in accordance with this Department's retention policy, unless determined to be of evidentiary value;
    c. Confirming, through random audits, that facial recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy; and
    d. Ensuring and documenting that personnel (including investigators from external agencies who request facial recognition searches) meet all prerequisites stated in this policy prior to being authorized to use the facial recognition system.

4. The Detroit Police Department is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this facial recognition policy or by the Department's facial recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

307.5 - 6.2 Weekly Report to the Board of Police Commissioners

The Crime Intelligence Unit 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. During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners.

307.5 - 6.3 Annual Report to the Board of Police Commissioners

The Crime Intelligence Unit shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the Department's facial recognition technology. The evaluation shall include if there were any relevant lawsuits or settlements involving facial recognition, the number of cases that use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

307.5 - 6.4 All Policy Changes to the Board of Police Commissioners

The Department shall seek the Board of Police Commissioners' approval regarding any and all changes to the Facial Recognition Policy.

307.5 - 7 Security and Maintenance

1. The Detroit Police Department will comply with generally accepted industry or other applicable standards for security to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related Department activity. The Department's facial recognition system will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to the Department's facial recognition information from outside the facility will be allowed only over secure networks. All results produced by the Department as a result of a facial recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

a. To whom it was released;
b. Date and time it was released; and
c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw it released).

2. All members with access to the Department's information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the local agency security officer (LASO), assigned to Technical Services, is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electric. Following assessment of the suspected or confirmed breach and as soon as practicable, the Department will notify the originating agency from which the entity received facial recognition information of the nature and scope of a suspected or confirmed breach of such information. The Department will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.
3. All facial recognition equipment and facial recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.
4. The Department will store facial recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.
5. Authorized access to the Department's facial recognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.
6. Usernames and passwords to the facial recognition system are not transferrable, must not be shared by Department members, and must be kept confidential.
7. The system administrator (Department LASO) will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).
8. Queries made to the Department's facial recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
9. The Department will maintain an audit trail of requested, accessed, searched, or disseminated facial recognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of facial recognition information for specific purposes and of what facial recognition information is disseminated to each individual in response to the request. Audit logs will include:

a. The name and unit of the law enforcement user;
b. The date of access;

c. Case number; and
d. The authorized law enforcement or public safety justification for access including a relevant case number.