PLANNING AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

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

TYPE OF DIRECTIVE: Manual Directive 307.5

SUBJECT: FACIAL RECOGNITION

ORIGINATED OR REQUESTED BY: Planning and Deployment

APPROVALS OR COMMENTS:
The above referenced directive is a new directive. The information in this directive was pulled by Planning and Deployment by five (5) other law enforcement agency's Facial Recognition policies (attached).

Approved
1/2/19

APPROVED
DEC 27 2018
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

Approved

APPROVED
JAN 11 2019
1ST ASSISTANT CHIEF
OFFICE OF THE CHIEF

RECEIVED
JAN 17 2019

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

42

Series	Effective Date	Review Date	Directive Number
300 Support Services		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 procedures for acceptable use of the images, information, and tools within the Detroit Police Department's facial recognition software and the Statewide Network of Agency Photos (SNAP) application.

307.5 - 2 POLICY

1. This policy was established to ensure that all images are lawfully obtained, including facial recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the Department. This policy also applies to the following:

    a. Images contained in a known identity face image repository and its related identifying information;
    b. The face image searching process;
    c. Any results from facial recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the Department; and
    d. Lawfully obtained probe images of unknown suspects that have been added to unsolved image files, pursuant to authorized criminal investigations.

2. Authorized Department members, personnel providing information technology services to the Department, private contractors, and other authorized users will comply with the Detroit Police Department's Facial Recognition Policy and will be required to complete training that is mandated through the Department's Crime Intelligence Unit. In addition, authorized Department members tasked with processing facial recognition requests and submissions must also complete specialized training mandated through the Department's Crime Intelligence Unit. 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. The Detroit Police Department will provide a printed or electronic copy of this facial recognition policy to the following:

   - Department members who provide facial recognition services;
   - Participating agencies; and
   - Individual authorized users.

d. All technology associated with facial recognition, including all related hardware and software support, is bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, particularly Policy Area 13, and the Michigan CJIS Security Addendum;
e. The information within the facial recognition databases is considered highly restricted personal information and personally identifiable information (PII) which may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security Policy, the Michigan CJIS Security Addendum, the CJIS Policy Council Act (1974 PA 163), MCL 28.211-28.216, and the most current CJIS Administrative Rules; and
f. Improper access, use, or dissemination of highly restricted personal information or PII obtained from the use of the Statewide Network of Agency Photos (SNAP) may result in criminal penalties and/or administrative sanctions. Criminal violations include, but are not limited to, those found in MCL 28.214 and MCL 257.903.

307.5 - 3 Definitions

307.5 - 3.1 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 - 3.2 Data Works

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

307.5 - 3.3 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.

307.5 - 3.4 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 - 3.5 Highly Restricted Personal Information
An individual's photograph or image, social security number, digitized signature, medical and disability information.

307.5 - 3.6 Mobile Facial Recognition (Mobile FR)
The process of conducting an automated FR search in a mobile environment.

307.5 - 3.7 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 - 3.8 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 - 4 Governance and Oversight
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;

d. 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. 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;
e. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;
f. 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
g. 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.

3. 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 - 5 Acquiring and Receiving Facial Recognition Information

1. The Detroit Police Department's facial recognition system can access and perform facial recognition searches utilizing all entity-owned facial image repositories.
2. The Detroit Police Department is authorized to access and perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP). These may include the following:

   a. Mug shot images;
   b. Driver's license photographs;
   c. State identification card photographs; and
   d. Sex Offender Registry.

3. For the purpose of performing facial recognition searches, authorized Department members will obtain probe images or accept probe images from authorized agencies for uses identified in this directive under section "Security and Maintenance."
4. Probe images will only be received from authorized law enforcement agencies in accordance with current memorandums of understanding established between this Department and the authorized entity involved. If a non-law enforcement entity wishes to submit a probe image for the purpose of a facial recognition search, the entity will be required to file an incident report with the appropriate law enforcement entity prior to the search.

5. The Detroit Police Department and, if applicable, any authorized requesting or participating agencies 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.

6. However, the Detroit Police Department accords special consideration to the collection of facial images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety. If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the DPD anticipates a need for the collection of facial images, the member assigned to vetting the event shall submit an Inter-Office Memorandum (DPD568), through channels, to the Department's Legal Advisor. The Legal Advisor will articulate whether collection of facial images by law enforcement officers at the event is permissible. The Inter-Office Memorandum (DPD568) shall include the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how facial images may be collected, used, or retained, in accordance with this policy, as appropriate. If facial images will be collected the plan will specify the type of information collection that is permissible, identify who will collect facials images (uniform or plainclothes members), and define the permissible acts of collection.
7. The use of mobile facial image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by the Chief of Police, or designee, in advance of the event. Facial images from a First Amendment-protected event will be used should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event.

307.5 - 6 Use of Facial Recognition Information

1. The Department's Crime Intelligence Unit shall provide assistance for ongoing criminal investigations and other types of inquiries.
2. Requests for facial recognition services shall be submitted, through channels, on an Inter-Office Memorandum (DPD568) to the commanding officer of Crime Intelligence, with photograph(s) or video(s) to be reviewed. Photograph(s) and video(s) shall be handled as specified in Manual Directive 306.1, Evidence Property.
3. If the facial recognition system detects a viable candidate, the Crime Intelligence Unit shall complete a supplemental incident report for the requestor. The supplemental

incident report shall contain the steps taken to compare the known and unknown photographs and how the examiner came to their conclusion.

4. In the event that a viable candidate cannot be located from the facial recognition system, the requestor will be notified that no candidate was identified.
5. If the Crime Intelligence Unit cannot discern a viable candidate, the photograph of the suspect will be considered unknown and remain in the facial recognition database system until:

   a. A viable candidate is found;
   b. The requestor notifies the Crime Intelligence Unit that the case has been completed, a viable candidate is no longer necessary, or the suspect has been found through other means; or
   c. The statute of limitations has expired for the specific case.

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, agency, and contact information of the law enforcement user;
    b. The date and time of access;
    c. Case number;
    d. Probe images;
    e. The specific information accessed;
    f. The modification or deletion, if any, of the facial recognition information; and
    g. The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available.

307.5 - 8 Accountability and Enforcement

307.5 - 8.1 Transparency

1. The Department will be open with the public with regard to facial recognition information collection, receipt, access, use, dissemination, retention, and purging practices.
2. The Department's facial recognition administrator (LASO) will be responsible for reviewing and responding to inquiries and complaints about the entity's use of facial recognition system, as well as complaints regarding incorrect information or privacy, civil rights, and civil liberties protections of the image repository maintained and facial recognition system accessed by the Department.

307.5 - 8.2 Accountability

1. The Department will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the facial recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to facial recognition information, may include any type of medium or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the facial recognition administrator pursuant to the retention policy. Audits may be complete by an independent third party or a designated representative. Appropriate elements of this audit process a key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.
2. Department members or other authorized users shall report errors, malfunctions, or deficiencies of facial recognition information and suspected or confirmed violations of the Department's facial recognition policy to the facial recognition administrator.
3. The facial recognition administrator will review and update the provisions contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the facial recognition system; the audit review; and public expectations.

307.5 - 8.3 Enforcement

1. Any authorized user who is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, may be subject to the following:

    a. Suspend or discontinue access to information;
    b. Apply appropriate disciplinary or administrative actions or sanctions; and/or
    c. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The Department reserves the right to establish the qualifications and number of personnel having access to the Department's facial recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this facial recognition policy.