NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL

CHAPTER: 51.1.1

TITLE: USE OF FACIAL RECOGNITION FOR CRIMINAL INVESTIGATIONS

EFFECTIVE: 10/02/2022
REVISED: NEW POLICY

PURPOSE

The purpose of this Chapter is to provide department members with guidelines for requesting access to facial recognition software for use in criminal investigations.

POLICY STATEMENT

1. Information gathering is a fundamental and essential element in the investigative duties of any law enforcement agency.

2. Facial recognition technology must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the Louisiana State Constitution, and applicable statutory authorities. The facial recognition process does not by itself establish a basis for a stop, probable cause to arrest, or to obtain an arrest or search warrant. However, it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

3. Facial recognition can be used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for the conviction or exoneration of suspects involved in a crime of violence or in cases of missing persons to identify or locate the missing person. **The individual results of the use of this technology alone are insufficient to constitute probable cause** but may be an element of reasonable suspicion or probable cause when viewed with other elements of the investigation to obtain an arrest or search warrant.

4. The safeguards and protocols built into this policy for the use of facial recognition technology mitigate the risk of biased law enforcement. This NOPD facial recognition policy integrates human investigators in all phases. All possible facial recognition matches undergo a peer review by other facial recognition investigators. Further, the possible match report includes the submitted image, and a notification stating that t**he 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.**

5. The approval, screening and use of any facial recognition function shall be assigned to specific members within the Investigation Support Division – Intelligence Unit of ISB by

the Captain of the Investigation Support Division. All members of the New Orleans Police Department are responsible for compliance with this Chapter.

6. All requests for use of or access to facial recognition software shall be made through the Investigation Support Division – Intelligence Unit of ISB. All requests shall be reviewed by the requesting investigator's supervisor and verified by the Intelligence Unit for appropriateness and conformance to the requirements of this Chapter and **Chapter 51.1 – Criminal Intelligence**. All requests for use of facial recognition (Form #357) shall be directed toward specific individuals where there is reasonable suspicion that said individuals may be planning, have engaged in, or are engaging in a crime of violence.

7. Use of facial recognition will be requested and authorized with due respect for the rights of those involved and disseminated only to those agencies or members authorized by law and only as appropriate for legitimate law enforcement purposes in accordance with the Constitution, Federal, State, and Municipal law and the procedures established in this Chapter. It is especially important that facial recognition not be used to suppress First Amendment rights, violate privacy, or otherwise adversely impact an individual's civil rights and civil liberties.

8. Information obtained using facial recognition that implicates or potentially implicates complicity of any public official in criminal activity or corruption shall be immediately reported to the Superintendent of Police.

9. The NOPD shall not use facial recognition technology to monitor and identify people in public gatherings or political rallies, except as provided in this chapter.

10. NOPD shall not use facial recognition technology as a surveillance tool.

11. NOPD Investigators shall not use facial recognition technology to authenticate an already identified subject or where identifiable information has been provided.

12. Facial recognition shall not be used for the investigation of a violation or attempted violation of any law criminalizing (1) abortion or the provision thereof by a licensed physician, and (2) any consensual sexual act between persons of the age of majority, including without limitation any law purporting to criminalize sexual contact between same-sex partners.

13. Facial recognition shall not be used for any internal administrative investigation .

14. The misuse of facial recognition technology will subject members to administrative and potentially criminal penalties.

DEFINITIONS

Crime of Violence— a felony involving the infliction or threatened infliction of serious bodily injury or death. (see RS 14:2(B)

Facial Recognition – is an automated or semi-automated system or process that displays the closest matches of a photograph, sketch or image uploaded to an image database and assists in identifying an individual, capturing information about an individual based on the physical characteristics of an individual's face. Used in combination with human analysis and additional investigation, facial recognition technology can serve as a valuable tool in solving crimes and increasing public safety.

Law Enforcement Purpose - the investigation, detection, analysis or enforcement of a crime or

a violation of law; operations associated with an AMBER, SILVER, BLUE or YELLOW alert; searches for missing persons, endangered persons or wanted persons; suspicious activity possibly related to terrorism or other public safety issue.

Reasonable Suspicion - specific, objective, articulable facts, within the totality of the circumstances, that, taken together with rational inferences, create a well-founded suspicion that there is a substantial possibility that a subject has engaged, is engaging, or is about to engage in criminal conduct.

Automated decision systems (also known as "ADS") - include any software, system, or process that aims to automate, aid, or **replace human decision making**. Automated decision systems can include both tools that analyze datasets to generate scores, predictions, classifications, or some recommended actions(s) that are used by agencies to make decisions that impact human welfare and the set of processes involved in implementing those tools.

Surveillance - the act of observing or analyzing the movements, behavior, or actions of identifiable individuals.

Fusion Centers - are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners.

REQUESTING USE OF FACIAL RECOGNITION SYSTEMS

15. Members who have an image relating to an individual they wish to identify in relation to a law enforcement purpose within the meaning of this Chapter, shall utilize **Form 357 – Facial Recognition Request Form** to document the request.

16. All requests shall be reviewed for appropriateness and approved by the requestor's immediate supervisor prior to sending to Investigation Support Division – Intelligence Unit of ISB for processing.

17. The use of facial recognition technology must be approved on a case-by-case basis by an NOPD supervisor. The NOPD Form 357, or its' electronic equivalent, will serve as a sworn affidavit certifying (a) the reason for the request and the enumerated crime justifying the use of facial recognition technology and (b) that all other reasonable means of identifying the individual have been exhausted, absent exigent circumstances.

18. Access to facial recognition technology is limited to NOPD facial recognition investigators. Facial recognition investigators are provided with direct access to facial recognition technology only after completing mandatory training related to the general use of the technology and image comparison principles, including the requirements of 28 CFR Part 23, Privacy, Civil Rights, and Civil Liberties Training.

19. The source of the image and underlying reasons for the requested use of facial recognition systems as an investigative lead shall be documented in an investigative report. The item number for that report shall be reflected in the request form. A copy of the form shall be included as an attachment to the report.

20. NOPD prohibits the use of facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

21. The results of the request shall also be documented in the same investigative report or a supplemental report as the original request item number.

22. No requests for the use of Facial Recognition Technology or access to information from a Fusion Center or any outside agency shall be made by any member directly to another jurisdiction, the State, or any federal agency without prior approval of the supervisor of the NOPD Intelligence Unit. All requests shall be reported to and tracked through NOPD – Investigation Support Division – Intelligence Unit of ISB and the Professional Standards Section.

RESPONSIBILITY FOR VETTING REQUESTS FOR FACIAL RECOGNITION SEARCHES

23. The Investigations & Support Bureau's (ISB) Investigation Support Division – Intelligence Unit of ISB has primary responsibility for:
    (a) Receiving requests from NOPD investigative units for the use of facial recognition for a law enforcement purpose.
    (b) Ensuring the submitted requests have been reviewed by the requestor's supervisor for appropriateness and compliance with this Chapter.
    (c) Processing the requests, if approved, through the facial recognition systems and databases to which NOPD has access by law or MOU.
    (d) Reviewing any responses received prior to release to the original requestor.
    (e) Forwarding the response to the original requestor when appropriate and within the guidelines of this Chapter.
    (f) Maintaining a record of all requests and the responses.

INVESTIGATIVE STANDARDS

24. The use of facial recognition for investigative purposes is a balance between information-gathering requirements for law enforcement and possible legal and privacy rights of individuals. To promote an equitable balance, members of this department shall adhere to the following:
    (a) Information gathering by use of facial recognition shall be premised on circumstances that provide a reasonable suspicion that specific individuals may be planning, have engaged, or are engaging in a specific crime of violence, sex crime, crime against a juvenile, or for a law enforcement purpose as defined in this Chapter, as governed by New Orleans Municipal Code Section 147-2. This can include:
        1. Identifying a crime victim or witness,
        2. Identifying a deceased person,
        3. Identifying an incapacitated person or one unable to identify themselves when exigent circumstances are present,
        4. Identifying an individual under arrest who does not possess a verifiable identification, is not forthcoming with identification or who appears to be using another's identity, identification, or false identification, and
        5. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism plot, etc.)
    (b) Investigative techniques employed shall be lawful and as minimally intrusive as necessary to gather enough information to prevent the criminal act and/or to identify and prosecute violators.
    (c) The Investigation Support Division – Intelligence Unit of ISB shall take reasonable steps to ensure that information regarding the use and access to facial recognition systems is relevant to an active, current, or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the requests for use of facial recognition and the source of all information received.

(d) Facial recognition shall not be used for the investigation of minor offenses, except as part of an investigation of a serious criminal offense.
(e) Information gathered and maintained by the New Orleans Police Department for law enforcement purposes may be disseminated only to those agencies or members authorized by law and only as appropriate for law enforcement purposes in accordance with the law and procedures established in this Chapter and **Chapter 51.1 – Criminal Intelligence**.
(f) A record shall be kept by the Investigation Support Division – Intelligence Unit of ISB regarding the dissemination of all such information to persons within the department or other law enforcement agencies.

COMPILING INFORMATION FROM FACIAL RECOGNITION SYSTEMS

25. Information gathering using facial recognition systems, as well as electronic, photographic, and related images shall be performed in a legally accepted manner and in accordance with procedures established by this department.

26. All information requests designated for the Investigation Support Division – Intelligence Unit of ISB shall be submitted, reviewed, and approved by the requesting officer's immediate supervisor prior to submission.

27. Members **shall retain official documentation relating to facial recognition only for purposes of their investigation** and as documented in a police report or official case file. Members shall not maintain documentation relating to facial recognition for personal reference or use.

ANALYSIS OF FACIAL RECOGNITION INFORMATION SUBMISSIONS

28. The Investigation Support Division – Intelligence Unit of ISB shall establish and maintain an internal process to ensure that information requested and gathered is reviewed and analyzed to derive its appropriateness and value in an investigation.

29. The review and analysis process should be accomplished by trained law enforcement personnel experienced in facial recognition procedures and criminal intelligence processes.

30. Images submitted and approved for comparison to a law enforcement repository of individuals that have been charged with a crime where a criminal court has jurisdiction that generate possible match candidates are manually reviewed by trained members of the ISD – Intelligence Unit or trained members of a U.S. Department of Homeland Security Designated Fusion Center to determine the differences between the submitted image and the possible matches.

31. If a possible match candidate is identified, the facial recognition investigator must then manually review and analyze each result. This process, known as facial identification, consists of visual comparison of the facial characteristics of each candidate against the submitted image. Comparisons are made with regard to various facial features such as the eyes, ears, nose, mouth, chin, lips, eyebrows, hair/hairline, scars, marks, and tattoos.

32. A possible match candidate is submitted for peer review by other facial recognition investigators. A supervisor of the facial recognition investigator performs a final review of a possible match candidate and provides final approval, if appropriate.

33. If there is a difference of opinion with the findings, the facial recognition investigators'

supervisor will direct personnel to continue investigation for a possible match candidate. A report of negative results will be provided to the requesting investigator if a possible match candidate is not identified or approved by the supervisor.

34. If a possible match candidate is approved, the facial recognition investigator will prepare a possible match report and attach it to the requesting investigator's request form. The possible match report includes the submission image, and **a notification stating that the 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.**

RECEIPT / EVALUATION OF INFORMATION

35. The following steps shall be taken to ensure the quality and reliability of facial recognition system information:
    (a) Information shall be evaluated with respect to reliability of the source and validity of the content. While evaluation may not be precise, this assessment must be made to the degree possible to guide others in using the information.
    (b) A record shall be kept of the source of all information where it is known.
    (c) Reports and other investigative material and information received by this department shall remain the property of the originating agency but may be retained by the New Orleans Police Department unless an MOU or CEA between NOPD and the source agency states otherwise.
    (d) Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another entity except with the consent of the originating agency.
    (e) Information having relevance to active cases or that requires immediate attention shall be forwarded to the responsible investigator or investigative unit supervisor as soon as possible.

36. Within 30 days of the request, investigators requesting the use of the technology must provide information in writing (by email notification or 105) to the Investigative Services Division and the Professional Standards Section a brief description of how the technology was used and whether the use of the technology successfully assisted with their investigation (i.e., led to an arrest or exoneration).

37. The Professional Standards Section Bureau shall be responsible for ensuring the following data is collected:

    (a) The total number of requests for the use of facial recognition technology.

    (b) For each request:
        i. the requesting officer's name and badge number;
        ii. the name of the NOPD supervisor approving the request and the date on which the request was granted;
        iii. the enumerated crime(s) justifying the request;
        iv. the age, gender, and race of the suspect;
        v. the accompanying NOPD item numbers;
        vi. whether the use of facial recognition technology resulted in a match; and
        vii. whether the use of facial recognition technology resulted in an arrest and/or charges.

CLASSIFICATION / SECURITY OF FACIAL RECOGNITION SYSTEMS

38. All requests and results will be “access level classified” to protect sources, investigations, and individual's rights to privacy and to provide a structure that will enable this department to control access to sensitive information.

39. These access level classifications shall be reevaluated whenever new information is added to an existing file or request for facial recognition system use.
    (a) **Restricted**—Files, requests or results that contain information that could adversely affect an ongoing investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the Intelligence Unit commander, Investigation Support Division of ISB Captain, ISB Deputy Chief or Superintendent of Police and only to authorized law enforcement members or agencies with a need and a right to know. Restrictions on the release and sharing of information in any multi-agency operation shall be governed by the Memorandum of Understanding or Cooperative Endeavor Agreement in place at the time.
    (b) **Confidential**—Files, requests or results that are less sensitive than restricted intelligence. It may be released to department personnel when a need and a right to know have been established by the Investigation Support Division of ISB Captain or his/her designee.
    (c) **Unclassified**—Files, requests or results that contain information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorized investigations that necessitate this information.

40. All restricted and confidential files shall be secured both physically and electronically, and access to all intelligence information shall be controlled and recorded by procedures established by the Specialized Investigations Division.

41. All files regarding facial recognition system requests shall be maintained in accordance with state and federal law.

42. All files regarding s facial recognition system requests released under freedom of information provisions or through disclosure shall be carefully reviewed and redacted as legal and appropriate.

AUDITING / PURGING FILES

43. The use of facial recognition systems and search requests shall be audited by the PSAB. Users will be required to provide appropriate justification for the use or request of facial recognition searches. PSAB shall have access to all documentation relating to facial recognition requests.

44. Appropriate justification will include the reason for the facial recognition system search, an NOPD Incident / Investigative Report and offense type. For searches conducted on behalf of another individual, the name and job title of the individual who requested the search will also be required.

45. The Captain of the division/district is responsible for ensuring that criminal intelligence files housed within that division/district are maintained in accordance with the law and the provisions of this Chapter and include information that is both timely and relevant.

46. All facial recognition system request files shall be audited and purged on an annual basis as established by the ISB Deputy Chief. Data utilized by MAX, or for ongoing investigations, shall be retained until it is anonymized, the investigation is concluded and/or any related judicial proceedings are final.

47. When a facial recognition system request file has no further information value and/or meets the legal criteria, it shall be destroyed in accordance with public records law.

48. A record of the purging of facial recognition system request files shall be maintained by the Investigation Support Division – Intelligence Unit of ISB for a minimum of seven (7) years after the purge.