NEW ORLEANS POLICE DEPARTMENT
OPERATIONS MANUAL

CHAPTER: 51.1.1

TITLE: FACIAL RECOGNITION AND CHARACTERISTIC TRACKING FOR CRIMINAL INVESTIGATIONS

EFFECTIVE: 10/02/2022
REVISED: DRAFT

PURPOSE

The purpose of this Chapter is to provide department members with guidelines for requesting access to facial recognition or characteristic tracking 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. Technology used to identify, locate, and track individuals 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.

3. Identifications made using facial recognition software may generate investigative leads through a combination of automated biometric comparisons and human analysis but do not establish a basis for a stop, or probable cause to arrest,

4. 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 authorized by this chapter and law, 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.

5. Any arrest, or request for an arrest warrant, must be supported by additional independent reliable evidence. Probable cause for an arrest or arrest warrant must be established using legally authorized methods other than Facial Recognition and should be based on a totality of the circumstances. Examples of other investigative methods may include, but are not limited to cellular data analysis; eyewitness testimony, DNA, etc.

6. Arrests, or requests for arrest warrants, shall not be made solely on the basis of an investigative lead developed through Facial Recognition Technology in combination with a lineup identification

7. 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 should undergo peer review by other facial recognition investigators. Further, the possible match report includes the submitted 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.**

8. The approval of the request or use of any facial recognition technology or characteristic tracking systems shall be provided in writing by an NOPD supervisor at the rank of Lieutenant or above, except as otherwise specified by this policy (approval via email is sufficient to meet the requirement of this paragraph).

9. All approvals for the use of facial recognition technology or characteristic tracking systems shall be made a part of the investigative case file and documented in an investigative report.

10. All requests for use of or access to facial recognition of characteristic tracking software shall be reviewed by the requesting investigator's supervisor and verified a Lieutenant for appropriateness and conformance to the requirements of this Chapter and law.

11. All requests for use of facial recognition to identify an unknown individual 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.

12. Requests for the use of facial recognition technology to identify an unknown individual shall be documented using the NOPD Form #357.

13. 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.

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

15. 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.

16. NOPD shall not use facial recognition technology to assist with locating an individual except in the following circumstances:

    (a) A valid arrest warrant exists ordering the apprehension of the individual who is attempting to be located;

    (b) An officer can establish reasonable articulable suspicion that immediately locating and detaining an individual is needed to prevent a crime that would cause serious bodily injury or death;

(c) To assist in the investigation of any of the crimes listed in New Orleans Municipal Code Section 147-2(d) with express approval from an NOPD Supervisor at the level of Lieutenant or above; or

(d) To locate a missing person.

17. 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.

18. Facial recognition technology shall not be used to identify or locate an individual for the sole purpose of determining someone's immigration status or for immigration enforcement.

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

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

DEFINITIONS

Automated decision systems (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.

Characteristic Tracking System - any software or system capable of tracking people and/or objects based on characteristics such as color, size, shape, age, weight, speed, path, clothing, accessories, vehicle make or model, or any other trait that can be used for tracking purposes, including BriefCam and similar software

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

Facial Recognition – an automated or semi-automated process that assists in identifying an individual and/or capturing information about an individual based on the physical characteristics of an individual's face.

Face or facial Surveillance – as provided by the Municipal Code of the City of New Orleans, means an automated or semi-automated process that uses facial recognition to scan individuals to assist in identifying, locating, or verifying the identity of an individual based on the physical characteristics of an individual's face.

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.

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 issues.

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.

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

REQUESTING OR USING FACIAL RECOGNITION SYSTEMS FOR IDENTIFICATIONS

21. 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.

22. All requests for identification using facial recognition systems shall be reviewed for appropriateness and approved by the requestor's immediate supervisor and/or a reviewing Lieutenant prior to submission to any authorized individual or entity for processing.

23. The use of facial recognition technology must be approved on a case-by-case basis by. 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.

24. Access to facial recognition technology is limited to NOPD facial recognition investigators or authorized entities through a written agreement. 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.

25. 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.

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

27. If facial recognition technology is used to identify a suspect, members may not conduct a lineup unless there is other evidence, in addition to the use of facial recognition technology, to support a belief that the suspect committed the crime under investigation.

REQUESTING OR USING FACIAL RECOGNITION TECHNOLOGY OR CHARACTERISTIC TRACKING SYSTEMS TO LOCATE AN INDIVIDUAL

28. NOPD shall work with the New Orleans Real Time Crime Center to ensure the submission or entry of any individuals into any system(s) used to locate individuals using facial recognition technology are consistent with this policy and the law.

29. All uses of characteristic tracking systems use proper video indexing and do not rely on or capture personally identifiable features.

30. All requests or uses of facial recognition technology or characteristic tracking systems for investigative purposes must be based on reasonable suspicion and be approved in writing by an NOPD supervisor at the rank of Lieutenant or above. Upon completion of the investigative need, any personally identifying data or biometric analysis data associated with the individual under investigation shall be removed from the system unless (1) a valid arrest warrant exists ordering the apprehension of the individual for a crime listed in New Orleans Municipal Code Section 147-2(d) and (2) that individual has not been located and arrested for the offense.

31. All requests or uses of facial recognition technology or characteristic tracking systems to locate a missing person shall be approved in writing by an NOPD supervisor at the rank of Lieutenant or above, unless there is a reasonable belief the individual is in imminent danger of death or serious bodily injury.

32. Members may request or use characteristic tracking systems to immediately locate and detain an individual for which reasonable articulable suspicion exists that immediate location and detention of that individual is needed to prevent a crime that would cause serious bodily injury or death.

33. When feasible, the use or request of characteristic tracking systems for the purpose outlined in the preceding paragraph must be expressly approved, preferably in writing, by an NOPD supervisor at the rank of Lieutenant or above. In any circumstance, the use of characteristic tracking systems shall be documented in an investigative report and properly logged into any systems feeding NOPD's dashboards.

34. All requests for and uses facial recognition technology or characteristic tracking systems, including through access to information from a Fusion Center, the Real Time Crime Center, or any outside entity, shall be logged into any systems feeding NOPD's dashboards, and shall include the following information:

(a) the requesting officer's name and employee ID number;
(b) the name of the NOPD supervisor approving the request
(c) the date on which the request was granted;
(d) the enumerated crime(s) justifying the request;
(e) the age, gender, and race of the suspect;
(f) the accompanying NOPD item numbers;
(g) whether the use of facial recognition technology for identification resulted in a match; and
(h) whether the use of the technology resulted in an arrest and/or charges.

RESPONSIBILITY FOR VETTING REQUESTS FOR FACIAL RECOGNITION USE

35. Each NOPD supervisor reviewing a request for the use of facial recognition technology or a characteristic tracking system has primary responsibility for:

(a) Ensuring the submitted requests are reviewed for appropriateness and compliance with this Chapter.
(b) Processing the requests, if approved, through the facial recognition systems and databases to which NOPD has access by law or MOU.
(c) Reviewing any responses received.
(d) Ensuring all uses and requests are thoroughly documented in an investigative report and the NOPD Technology use tracking log.

INVESTIGATIVE STANDARDS

36. 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 technology or characteristic tracking systems 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. When an officer can establish reasonable articulable suspicion that immediately locating and detaining an individual is needed to prevent a crime that would cause serious bodily injury or death;
6. To locate a missing person,
7. To locate an individual for which a valid arrest warrant exists ordering the apprehension of that individual for crimes listed in New Orleans Municipal Code Section 147-2(d),
8. To assist in the investigation of any of the crimes listed in New Orleans Municipal Code Section 147-2(d) with express approval from an NOPD Supervisor at the level of Lieutenant or above; or

(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) NOPD supervisors 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.

(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 in the investigative case file by the investigator regarding the dissemination of all such information to persons within the department or other law enforcement agencies.

COMPILING INFORMATION FROM FACIAL RECOGNITION TECHNOLOGY OR CHARACTERISTIC TRACKING SYSTEMS

37. 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.

38. Any 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.

39. 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

40. Any review and analysis process conducted by NOPD members to identify an individual using facial recognition technology should be accomplished by trained law enforcement personnel experienced in facial recognition procedures and criminal intelligence processes.

41. Images submitted and approved for comparison to a law enforcement repository of individuals charged with a crime that generate possible match candidates require manual review by trained members of the NOPD or an authorized entity to determine the differences between the submitted image and the possible matches.

42. 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.

43. A possible match candidate should be 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.

44. 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 reviewing member's supervisor.

45. 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

46. 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.

47. Within 30 days of the request, investigators requesting the use of the technology must update their case file to ensure NOPD's dashboard information properly reflects the following if applicable:

(a) whether the use of facial recognition technology for identification resulted in a match; and

(b) whether the use of the technology resulted in an arrest and/or charges.

48. In the event an arrest is not made through the use of facial recognition technology or characteristic tracking software within 30 days, the NOPD dashboards shall be updated with information from the arresting or investigating officer once the subject has been arrested.

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

(a) The total number of requests for and uses of facial recognition technology.

(b) For each request:

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

CLASSIFICATION / SECURITY OF FACIAL RECOGNITION SYSTEMS

50. 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.

51. 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 their 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.

52. 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.

53. All files regarding facial recognition technology or characteristic tracking system requests shall be maintained in accordance with state and federal law.

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

AUDITING / PURGING FILES

55. The use of facial recognition technology or characteristic tracking 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.

56. Appropriate justification will include the reason for the 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.

57. 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.

58. 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.

59. 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.

60. A record of the purging of facial recognition system request files shall be maintained by the Professional Standards and Accountability Bureau for a minimum of seven (7) years after the purge.