The City of New York
Department of Investigation

NADIA I. SHIHATA
COMMISSIONER

180 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

**Release #35-2026**
**nyc.gov/doi**

**FOR IMMEDIATE RELEASE**
**TUESDAY, NOVEMBER 17, 2026**

**CONTACT: DIANE STRUZZI**
**CLODAGH MCGOWAN**
**(212) 825-5931**

# DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD ISSUES REPORT ASSESSING THE NYPD'S COMPLIANCE WITH THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT FOCUSING ON FACIAL RECOGNITION TECHNOLOGY POLICIES AND ISSUING 17 RECOMMENDATIONS

Nadia I. Shihata, Commissioner of the New York City Department of Investigation ("DOI"), issued the following report from DOI's Office of the Inspector General for the New York City Police Department ("OIG-NYPD") concerning the New York City Police Department's ("NYPD") compliance with the Public Oversight of Surveillance Technology ("POST") Act. For this Report, the fourth published pursuant to the POST Act,[1] DOI's OIG-NYPD reviewed NYPD's Impact and Use Policy ("IUP") for facial recognition technology, a topic addressed in its inaugural POST Act report in 2022. In August 2025, OIG-NYPD decided to focus on the issue after receiving a letter from the Legal Aid Society requesting an investigation of alleged violations of the NYPD's facial recognition IUP. Following its Post Act review, DOI's OIG-NYPD issued 17 recommendations to the NYPD, finding that while the NYPD largely complies with the POST Act with respect to its facial recognition policies, there are a series of changes and refinements that the NYPD should make to its procedures to further transparency interests and to allow for more accurate and controlled use of facial recognition technology, including modifications to address instances where the NYPD violated its own policy and failed to comply with recently enacted legislation. The Report follows this release and can be found at this link: OIG-NYPD Reports

DOI Commissioner Nadia I. Shihata said, "In examining the NYPD's Facial Recognition Impact and Use Policy, DOI's OIG-NYPD found there is room for the NYPD to strengthen transparency and control of the Department's use of this significant surveillance technology. While surveillance technology can be an important tool relied on by law enforcement, its use must be accompanied by public transparency, policies, and procedures to limit the risk of misuse and protect civil rights. The 17 recommendations that DOI's OIG-NYPD has issued as a result of this examination will help the NYPD achieve this goal and provide the public with greater insight into the use of this technology."

OIG-NYPD first addressed the NYPD's use of facial recognition technology in its 2022 inaugural POST Act report, which made two recommendations regarding the NYPD's use of facial recognition technology; specifically, that (1) the NYPD adopt guidelines outlining how and when the images input into facial recognition programs could be modified; and (2) the NYPD periodically audit its compliance with its own facial recognition policies. While the NYPD rejected both recommendations, they were subsequently enacted legislatively by the New York City Council in 2025, requiring the NYPD to implement the changes either immediately or as effective on September 1, 2025.

[1] The three previous Post Act reports by DOI's OIG-NYPD
- An Assessment of NYPD's Response to the POST Act, November 3, 2022
- An Assessment of NYPD's Compliance with the POST Act, May 30, 2024
- An Assessment of NYPD's Compliance with the POST Act, December 18, 2024

The NYPD has two policy and procedure documents related to the use of facial recognition technology: (1) its Facial Recognition Impact and Use Policy, which was most recently updated in February 2026 and includes several addenda; and (2) Patrol Guide § 212-129, titled "Facial Recognition Technology," which has been effective since December 2, 2022, and sets forth the NYPD's internal procedures for the use of facial recognition technology.

The POST Act requires DOI to prepare annual audits of the NYPD's surveillance technology IUPs, including: (1) assessment of the NYPD's compliance with the terms of its own policies; (2) descriptions of any known or reasonably suspected violations of the policies; and (3) recommendations on revisions to the IUPs. To conduct this audit, OIG-NYPD performed a section-by-section analysis of the most recent version of the Facial Recognition IUP, published in February 2026. OIG-NYPD then compared the Facial Recognition IUP against the NYPD's internal procedures and practices regarding the use of facial recognition technology embodied in a provision of the NYPD's Patrol Guide, as described during interviews of NYPD officials about its use of facial recognition technology, and as reflected in other information provided by the NYPD. Finally, OIG-NYPD further informed its findings through a review of publicly available news and research articles regarding facial recognition technology.

This Report offers the NYPD 17 recommendations concerning its Facial Recognition IUP that will improve the NYPD's compliance, particularly with recent amendments to the POST Act passed in 2025. Nine recommendations propose updates to the IUP to ensure alignment with the POST Act. The remaining eight recommendations focus on enhancing the operational efficacy of the NYPD's facial recognition processes, both internally and in its coordination with outside entities. Notably, while the time period of this Report covers data, information, and policies in effect through 2025, OIG-NYPD became aware of changes to certain policies and procedures discussed herein only after the NYPD received the Report for comment. OIG-NYPD has included these updates in the Report to avoid redundancy in its recommendations, ensuring they remain relevant.

The Recommendations OIG-NYPD issued to NYPD are:

**Recommendation #1:** The NYPD should amend the Facial Recognition Impact and Use Policy to include the names of the three facial recognition products in use at the NYPD.

**Recommendation #2:** The NYPD should amend the Facial Recognition Impact and Use Policy to enumerate the photo repositories associated with each of the facial recognition products it uses, as well as to identify specifically from where the photographs contained in the photo repositories are obtained.

**Recommendation #3:** The NYPD should amend its Facial Recognition Impact and Use Policy to specifically identify which Bureaus have access to facial recognition technology, what those Bureaus do, and who they serve.

**Recommendation #4:** The NYPD should update Patrol Guide 212-129 to instruct personnel to request facial recognition analysis only from the authorized unit within their assigned Bureau.

**Recommendation #5:** The NYPD should ensure that facial recognition analysis logs in both the Enterprise Case Management System and the Intelligence Division Case Management System are standardized to capture consistent and accurate data collection across all entries.

**Recommendation #6:** The NYPD should update Patrol Guide 212-129 to memorialize the Facial Recognition Impact and Use Policy's guidelines regarding acceptable image enhancement techniques.

**Recommendation #7:** The NYPD should establish and document an authorization process requiring facial recognition investigators to obtain permission from the Chief of Detectives or Chief of Intelligence (depending on the relevant Bureau the facial recognition investigator is assigned to) prior to editing probe images beyond standard parameters.

**Recommendation #8:** The NYPD should implement a mandatory documentation process to log all probe image modifications in compliance with the 2025 POST Act amendments.

**Recommendation #9:** The NYPD should amend the Facial Recognition Impact and Use Policy and Patrol Guide 212-129 to include guidance on how to select which facial recognition software program to use when conducting facial recognition analyses.

**Recommendation #10:** The NYPD should amend the Facial Recognition Impact and Use Policy, Patrol Guide 212-129, and other related policies to (1) clearly indicate which individual(s) in the Intelligence and Counterterrorism Bureau are authorized to review facial recognition analysis requests to outside agencies; and (2) require formal documentation of the outside request process in both the Detective Bureau and the Intelligence and Counterterrorism Bureau, including whether each request was approved or denied along with the reasoning behind the decision.

**Recommendation #11:** The NYPD should amend the Facial Recognition Impact and Use Policy and all associated policies to require mandatory supervisory review and blind peer review for all facial recognition analyses, and to mandate the documentation of reviewer names and result outcomes.

**Recommendation #12:** The NYPD should update the Facial Recognition Impact and Use Policy and related policies to codify procedures for facial recognition requests performed by outside entities, establish guidelines for officers' use of the results, and ensure that this process is documented and auditable.

**Recommendation #13:** The NYPD should adopt procedures in Patrol Guide 212-129 sufficient to ensure that FIS and the Intelligence Division do not process the same outside facial recognition requests.

**Recommendation #14:** The NYPD should provide training on the operation of facial recognition technology and related NYPD policies regarding the use of such technology to all investigators authorized to conduct searches.

**Recommendation #15:** The NYPD should establish recertification requirements involving additional training at periodic intervals for its facial recognition investigators.

**Recommendation #16:** The NYPD should adopt a policy requiring annual audits of its facial recognition analyses in accordance with the 2025 amendments to the POST Act and amend the Facial Recognition Impact and Use Policy consistent with the new policy.

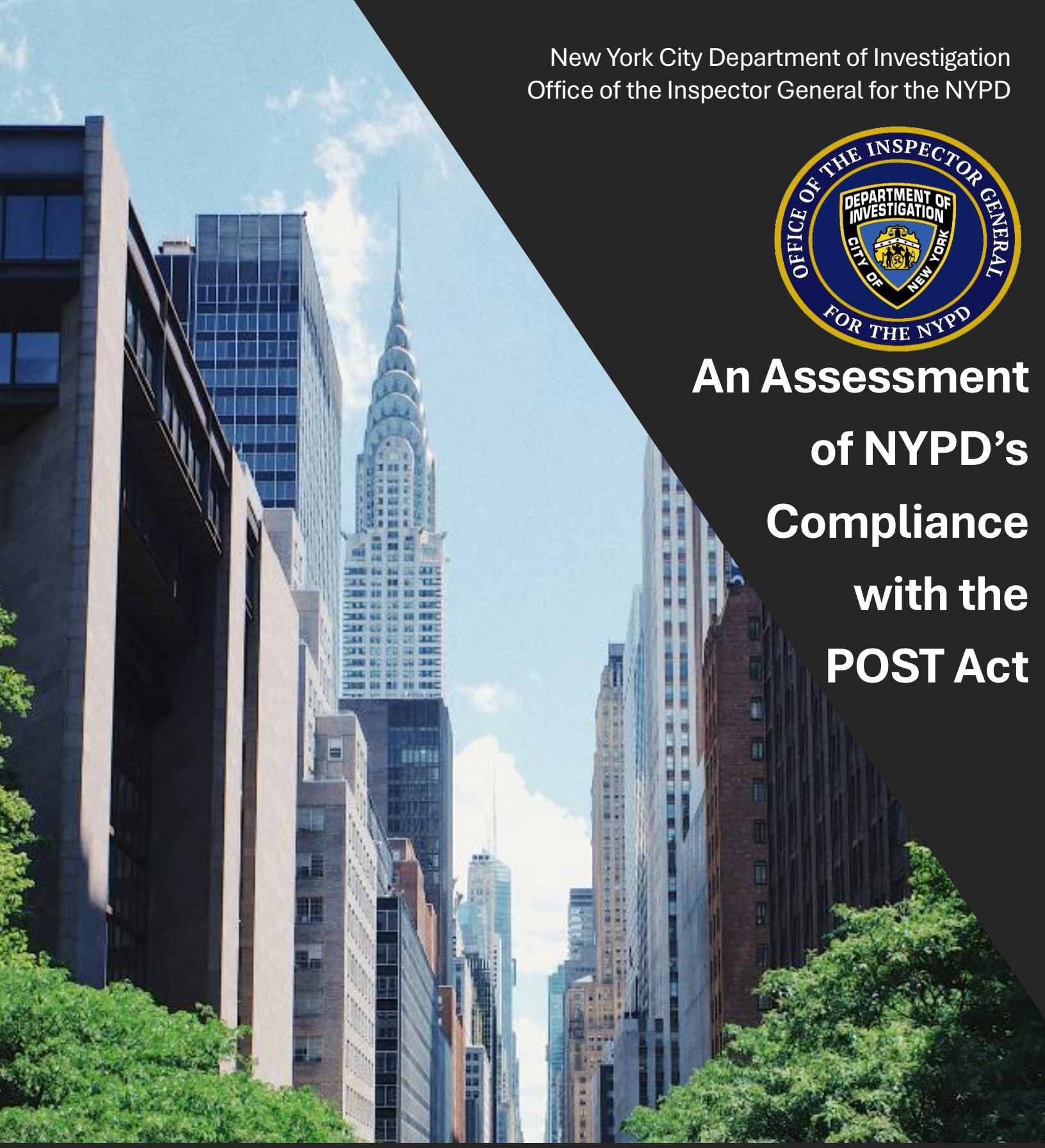
**Recommendation #17:** The NYPD should regularly review its facial recognition technology vendor's National Institute of Standards and Technology evaluations to verify ongoing performance consistency.

Commissioner Shihata thanked NYPD Commissioner Jessica S. Tisch, and her staff, for their cooperation on this Report.

At DOI, this investigation was conducted by Senior Investigative Analyst Marin Lucic in DOI's Office of the Inspector General for NYPD, under the supervision of Deputy Inspector General Lesley Bedeau, Special Counsel to the Inspectors General Maria Kostel, Acting Inspector General Christina Soto, and Acting First Deputy Commissioner Christopher Ryan, with assistance from Special Investigative Counsel Zachary Bannon.

*DOI is one of the oldest law-enforcement agencies in the country and New York City's corruption watchdog. Investigations may involve any agency, officer, elected official or employee of the City, as well as those who do business with or receive benefits from the City. DOI's strategy attacks corruption comprehensively through systemic investigations that lead to high-impact arrests, preventive internal controls and operational reforms that improve the way the City runs.*

**DOI's press releases can also be found at twitter.com/NYC_DOI**
**Know something rotten in City government? Help DOI Get the Worms Out of the Big Apple.**
**Call: 212-3-NYC-DOI or email: Corruption@DOI.nyc.gov**



New York City Department of Investigation
Office of the Inspector General for the NYPD

# An Assessment of NYPD's Compliance with the POST Act

November 2026

**Nadia I. Shihata,** Commissioner

**Christina Soto,** Acting Inspector General

## Table of Contents

**I. Introduction and Executive Summary 1**

**II. Background on the Use of Facial Recognition in Law Enforcement 2**

**III. The POST Act's Framework for Surveillance Policy and Oversight 5**

**IV. Assessment of the NYPD's Facial Recognition Impact and Use Policy 8**

A. Description of the Capabilities of the NYPD's Facial Recognition Technology 8

B. Uses and Restrictions on the Use of Facial Recognition Technology 11

*1. Who Has Access to Facial Recognition Technology?* 13

*2. What Is the Process for Conducting Facial Recognition Analysis?* 15

*3. Can "Probe Images" Be Modified Before Use?* 18

*4. How are Photo Repositories and Software Products Selected for Facial Recognition Analysis?* 20

*5. How are Peer and Supervisor Reviews Conducted?* 22

*6. How are Other Use Restrictions Implemented?* 23

C. The Prevention of Unauthorized Access 24

D. The Retention, Access, and Use of Data 25

E. The Use of Data by Members of the Public 26

F. Disclosure to Outside Entities 27

G. The Training of Facial Recognition Investigators 29

H. Internal Audit and Oversight Mechanisms 30

I. Health and Safety Effects 31

J. Potential Disparate Impacts 32

**V. Conclusion 33**

**Appendix A: Legal Aid Society Letter 36**

**Appendix B: NYPD's Facial Recognition IUP – February 2026 40**

**Appendix C: Patrol Guide 212-129, Facial Recognition Technology 52**

## I. Introduction and Executive Summary

The Public Oversight of Surveillance Technology ("POST") Act of 2020 requires the New York City Police Department ("NYPD") to publish documents describing how it uses surveillance technologies and their impacts, and to solicit public comment on these documents, known as Impact and Use Policies ("IUPs").[1] The POST Act assigns the New York City Department of Investigation ("DOI") responsibility for auditing NYPD's compliance with its IUPs, ensuring that surveillance technologies are used only as described and providing recommendations for improving the policies.[2]

One of the driving concerns that led to the passage of the POST Act was the NYPD's use of facial recognition technology ("FRT").[3] Concerns about facial recognition technology remain present to this day. On August 25, 2025, the Office of the Inspector General for the NYPD ("OIG-NYPD") received a letter from the Legal Aid Society alleging that the NYPD had violated its facial recognition IUP ("the Policy" or "the Facial Recognition IUP") on at least two occasions, one of which allegedly resulted in the arrest of an individual who did not commit the charged crime. The alleged IUP violations related to comparing probe images to images outside the NYPD's authorized photo repositories and relying on facial recognition analysis conducted by outside entities. In the letter, the Legal Aid Society "request[ed] that [OIG-NYPD] conduct an expeditious and thorough investigation into the NYPD's facial recognition policies and any methods employed to circumvent its own policies."[4] The two occasions discussed in the Legal Aid Society's letter resulted in criminal cases that were ultimately dismissed and sealed in June and July 2025, preventing the Office from accessing relevant information. As a result, OIG-NYPD was unable to make findings regarding either of the specific cases discussed in the Legal Aid Society's letter, though in one case written judicial findings made in connection with a dismissal motion substantiate the Legal Aid Society's claims.[5] OIG-NYPD decided to focus the 2025 POST Act report on the NYPD's Facial Recognition Impact and Use Policy.

OIG-NYPD first addressed the NYPD's use of facial recognition technology in its 2022 inaugural POST Act report, which made two recommendations regarding the NYPD's use of facial recognition technology; specifically, that (1) the NYPD adopt guidelines outlining how and when the images input into facial recognition programs could be modified; and (2) the NYPD periodically audit its compliance with its own

[1] *See* N.Y.C. LOCAL LAW No. 65 of 2020 § 1. Sections governing the NYPD are codified at N.Y.C. ADMIN. CODE § 14-188.
[2] *See* N.Y.C. LOCAL LAW No. 65 of 2020 § 2. Sections governing DOI are codified at N.Y.C. CHARTER § 803(c-1).
[3] *See* N.Y.C. Council, *Committee Report of the Justice Division* at 9 (June 18, 2020), *available at* https://legistar.council.nyc.gov (last visited May 19, 2026).
[4] Appendix A at 3.
[5] *See People v. Zuhdi A.*, 86 Misc. 3d 1227(A) (N.Y. Sup. Ct. 2025), *available at* https://www.nycourts.gov/reporter/3dseries/2025/2025_51047.htm (last visited Nov. 9, 2026).

facial recognition policies.[6] While the NYPD rejected both recommendations, both were subsequently enacted legislatively by the New York City Council in 2025 requiring the NYPD to implement the changes either immediately or as effective on September 1, 2025.[7]

While OIG-NYPD's review found that the NYPD largely complies with the POST Act with respect to its facial recognition policies, OIG-NYPD also concluded that there are a series of changes and refinements that the NYPD should make to its procedures to further transparency interests and to allow for more accurate and controlled use of facial recognition technology, including modifications to address instances where the NYPD violated its own Policy or failed to comply with recently enacted legislation. Accordingly, OIG-NYPD is issuing seventeen Policy and Procedure Recommendations to improve the NYPD's compliance in this regard. Nine recommendations propose updates to the Impact and Use Policy to ensure alignment with the POST Act. The remaining eight recommendations focus on enhancing the operational efficacy of the NYPD's facial recognition processes, both internally and in its coordination with outside entities. Notably, while the time period of this Report covers data, information, and policies in effect through 2025, OIG-NYPD became aware of changes to certain policies and procedures discussed herein only after the NYPD received a draft of this Report for comment. OIG-NYPD has included these updates in the Report to avoid redundancy in its recommendations, ensuring they remain relevant.

This Report proceeds in three substantive parts. First, it discusses the use of facial recognition technology in varying law enforcement environments, including an overview of the positions commonly stated in favor and against its use in law enforcement. Second, it summarizes the requirements of the POST Act as they pertain to the use of facial recognition technology. And third, it examines the NYPD's Impact and Use Policy for facial recognition technology and whether the NYPD complies with the Policy and recent legislative amendments to the POST Act, offering recommendations to bring NYPD into compliance with recently enacted law and its own Policy.

## II. Background on the Use of Facial Recognition in Law Enforcement

Facial recognition analysis is a digital process that enables the detection, analysis, and comparison of human faces from images to confirm identities or recognize individuals.[8] Facial recognition is a specific application of artificial

[6] *See* N.Y.C. DEPT. OF INVESTIGATION, OFFICE OF THE INSPECTOR GEN. FOR THE NYPD, *An Assessment of NYPD's Response to the POST Act*, 21 (Nov. 2022), available at https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf (last visited Aug. 8, 2026).

[7] *See* N.Y.C. LOCAL LAWS No. 54 to 56 of 2025.

[8] *See* Michael Christopher Naughton, *Considering Face Value: The Complex Legal Implications of Facial Recognition,* A.B.A. CRIM. JUST. MAG. (Jan. 30, 2025), *available at* https://www.americanbar.org/groups/criminal_justice/resources/magazine/2025-winter/face-value-complex-legal-implications-facial-recognition-tech/ (last visited May 16, 2026).

intelligence, using machine learning and deep learning algorithms to detect faces, extract facial features, and compare those features against stored biometric data.[9] By learning patterns from thousands or millions of facial images, these algorithms can recognize and match complex facial features. The accuracy of facial recognition algorithms is improved by varying the aspects of a facial image that are being measured and evaluated. This includes varying the demographics of subjects (e.g. age, race, gender, etc.), lighting conditions, angles, and more.[10]

There are two primary uses of facial recognition technology: verification (one-to-one, or 1:1) and identification (one-to-many). Verification involves comparing an image of a known individual to a single reference image to verify identity, similar to how smartphones use facial recognition to unlock a user's phone in lieu of a passcode. Identification involves attempting to determine the identity of an unknown individual by comparing their image against a larger database of images.[11] The NYPD's uses of facial recognition fall into the latter "identification" category.

When used by law enforcement, facial recognition algorithms typically follow a four-stage process.[12] First, the algorithm detects a face within an image (known as a "probe image"). Second, it creates a geometric map of the face by measuring its dimensions, which then converts into a string of numbers referred to as a "faceprint."[13] Third, an artificial intelligence model attempts to confirm or recognize a person's identity within the image by cross-referencing the image against other faceprints within a larger photo repository.[14] Fourth, once the probe image is matched with an image in the photo repository, a trained member of a law enforcement agency reviews and then approves or rejects any match proposed by the technology.[15]

Currently, almost nine hundred law enforcement agencies in the United States use facial recognition technology.[16] The extent to which facial recognition is used depends in part on the degree to which it is regulated in a jurisdiction. There are no federal laws regulating the development or use of facial recognition technology, but

---

[9] *Id.*
[10] *Id.*
[11] *See* Rochelle M. Garza, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology,* U.S. COMM'N ON CIV. RTS. (Sept. 19, 2024), *available at* https://www.usccr.gov/reports/2024/civil-rights-implications-federal-use-facial-recognition-technology (last visited Jul. 7, 2026).
[12] *See* Michael Christopher Naughton, *Considering Face Value: The Complex Legal Implications of Facial Recognition,* A.B.A. CRIM. JUST. MAG. (Jan. 30, 2025), *available at* https://www.americanbar.org/groups/criminal_justice/resources/magazine/2025-winter/face-value-complex-legal-implications-facial-recognition-tech/ (last visited May 16, 2026).
[13] *Id.*;
[14] *Id.;*
[15] *Id.;*
[16] *See* Atlas of Surveillance Database, https://www.atlasofsurveillance.org/search?location=&technologies%5Bface-recognition%5D=on&sort= (a project of the Electronic Frontier Foundation that is publicly available and tracks the deployment of multiple surveillance technologies by law enforcement agencies around the United States) (last visited May 19, 2026).

state and local practices vary dramatically.[17] Some jurisdictions impose no restrictions. Others, like San Francisco, have imposed outright bans.[18] New York City lies between these two poles, imposing requirements that the NYPD develop and adhere to internal policies regarding facial recognition.[19] At the federal level, the Department of Defense, Department of Health and Human Services, Department of Homeland Security, Department of the Interior, Department of Justice ("DOJ"), and Department of the Treasury have all reported using facial recognition technology. For example, the Federal Bureau of Investigation ("FBI") and the United States Marshals Service use facial recognition to generate leads and locate suspects; while the Department of Homeland Security uses facial recognition at airports and land borders to verify traveler identities.[20]

The rapid increase in the use of facial recognition technology across police departments nationwide has elicited passionate responses ranging from enthusiastic support to admonition.[21] Supporters praise facial recognition technology's benefit to law enforcement agencies, including its ability to increase the efficiency of suspect identification.[22] A 2024 DOJ report notes that facial recognition technologies "can be faster and more efficient than other investigative methods" when used to identify and locate missing persons or to identify deceased or incapacitated individuals.[23] A 2024 study on the effect of facial recognition technology on violent crime outcomes in the United States found that cities that implemented police facial recognition systems saw decreases in violent crime and homicide rates compared to cities that had not adopted the technology.[24] The study did not find evidence that facial recognition use

---

[17] *See* Maria Eira, et al., *A Policy Framework for Responsible Limits on Facial Recognition, Use Case: Law Enforcement Investigations,* WORLD ECON. F. (Nov. 2022), 25, *available at* https://www.weforum.org/publications/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case- law enforcement-investigations-revised-2022/ (last visited Feb. 26, 2026).

[18] *See* S.F., CAL., ADMIN. CODE § 107-19; *See also* S.F., CAL., ADMIN. CODE §19B.2 (d).

[19] *See* N.Y.C. ADMIN. CODE § 14-188.

[20] *See* Rochelle M. Garza, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology,* U.S. COMM'N ON CIV. RTS. (Sept. 19, 2024), *available at* https://www.usccr.gov/reports/2024/civil-rights-implications-federal-use-facial-recognition-technology (last visited Jul. 7, 2026).

[21] *See* Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH. POL'Y PRESS (Jan. 6, 2025), *available at* https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ (last visited May 16, 2026).

[22] *See* George-Marius Tical, *Facial Recognition and Biometric Systems: Benefits and Challenges for Law Enforcement,* XXX 2(18) LAND FORCES ACAD. REV., *available at* https://reference-global.com/download/article/10.2478/raft-2025-0024.pdf (last visited Apr. 12 , 2026); T.J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 862 (May 11, 2022), *available at* https://scholarlycommons.law.wlu.edu/wlulr/vol79/iss2/7/ (last visited Dec. 13, 2025).

[23] *Artificial Intelligence and Criminal Justice,* U.S. DEPT. OF JUST., 16, (Dec. 3, 2024), *available at* https://www.justice.gov/olp/media/1381796/dl?inline (last visited Jan. 6, 2026).

[24] *See* Thaddeus L. Johnson, et al., *Police facial recognition applications and violent crime control in U.S. cities*, 155 105472 CITIES (Dec. 2024), *available at* https://doi.org/10.1016/j.cities.2024.105472 (last visited Mar. 8, 2026).

caused racial disparities in arrests, nor evidence that the use of facial recognition increased the likelihood of over-policing.[25]

Critics of facial recognition technology often cite concerns about privacy, mass surveillance, and lack of transparency by law enforcement agencies.[26] Facial recognition systems collect and store biometric facial data derived from images such as photos or videos. This data includes facial images, facial landmarks (key points on the face such as distance between the eyes or shape of the jawline), and facial templates (a mathematical representation of a face). Sensitive information stored as part of a facial recognition system is susceptible to data breaches in which confidential information can be accessed, disclosed, or stolen without authorization.[27] Issues have also been raised regarding facial recognition's accuracy and propensity to lead to disparate racial impacts.[28]

## III. The POST Act's Framework for Surveillance Policy and Oversight

First enacted in 2020 and amended in 2025, the POST Act sets the framework under which the NYPD must set and disclose its policies for the use of surveillance technology, including facial recognition technology.[29] The POST Act also establishes

---

[25] *Id.* at 1 and 10.

[26] *See* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology,* ELEC. FRONTIER FOUND., (Feb. 12, 2018), *available at* https://www.eff.org/wp/ law enforcement-use-face-recognition (last visited Nov. 12, 2025); *See also* Lachlan Urquhart & Diana Miranda, *Policing Faces: The Present and Future of Intelligent Facial Surveillance*, 31(2) INFO. & COMMC'N TECH. L., 194, 219 (2021), *available at* https://www.tandfonline.com/doi/full/10.1080/13600834.2021.1994220 (last visited Nov. 12, 2025).

[27] *See* Emily Vetter, *2.9 Billion Records, Including Social Security Numbers, Stolen in Data Hack: What to Know,* USA TODAY, (Aug. 15, 2024), *available at* https://www.usatoday.com/story/tech/2024/08/15/social-security-hack-national-public-data-breach/74807903007/ (last visited Nov. 12, 2025); *See also* Jordan Pearson, *A Face Recognition Firm that Scans Faces for Bars Got Hacked-and that's Just the Start,* WIRED, (May 2, 2024), *available at* https://www.wired.com/story/outabox-facial-recognition-breach/(last visited Nov. 12, 2025); *See also* Eyewitness News, *Cyberattack exposes sensitive data on NYC public school students, staff,* ABC 7 N.Y, (Jun. 23, 2023), https://abc7ny.com/post/nyc-doe-data-breach-department-of-education-cyberattack-public-schools/13420314/ (last visited Nov. 12, 2025); *See also* Thora Knight, Steven Stransky, & Thomas F. Zych, *New York Data Breach Law Amended: New Timelines and Expanded Regulatory Reporting,* THOMPSON HINE LLP, (Jan. 2, 2025), *available at* https://www.thompsonhine.com/insights/new-york-data-breach-law-amended-new-timelines-and-expanded-regulatory-reporting/ (last visited Nov. 12, 2025).

[28] *See, e.g.*, Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES (Aug. 6, 2023), *available at* https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html (last visited May 19, 2026); *See also* Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), *available at* https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ (last visited Nov. 12, 2025); Amnesty International Press Release, *New Research Finds Facial Recognition Technology is Reinforcing Racist Stop-and-Frisk Policing in New York* (Feb. 14, 2022), *available at* https://www.amnestyusa.org/press-releases/facial-recognition-technology-reinforcing-racist-policing-new-york/) (last visited Nov. 12, 2025).

[29] *See* N.Y.C. LOCAL LAW No. 65 of 2020; *See also* N.Y.C. LOCAL LAWS No. 54 to 56 of 2025. Codified as it relates to the NYPD in N.Y.C. ADMIN. CODE §§ 14-188 and 14-188.1.

DOI's role in evaluating the NYPD's compliance with both the POST Act and its own policies promulgated pursuant to the Act.[30]

Pursuant to the Act, the NYPD is required to publish a proposed Impact and Use Policy "at least ninety days prior to the use of any new and distinct surveillance technology," defined as a system capable of collecting and utilizing audio, video, location, thermal, biometric, or similar information.[31] The public is entitled to comment on a proposed Impact and Use Policy for 45 days after its publication, after which the NYPD Commissioner must consider the public comments for no more than 45 days before publishing a final Impact and Use Policy.[32] Impact and Use Policies are written documents, which must include ten categories of information about a technology:

1. A description of the technology's capabilities;
2. NYPD rules and guidelines regulating access to and use of the technology, including use prohibitions and restrictions;
3. Safety measures in place to protect information collected by the technology from unauthorized access;
4. Policies relating to the retention, access, and use of data collected by the technology;
5. Policies relating to the access or use of data collected by the technology by members of the public;
6. The names of all entities outside the NYPD that have access to the data collected by the surveillance technology, including the type of information that may be disclosed to the entity and the safeguards imposed by the NYPD on the entity's use and dissemination of the information;
7. Whether training is required by the NYPD for an individual to use the technology or access information collected by it.
8. A description of internal audit and oversight mechanisms within the NYPD that ensure compliance with the Impact and Use Policy;
9. Any tests or reports regarding the health and safety effects of the technology and any information about the physical safety hazards presented by it;

[30] Sections of the POST Act relevant to DOI are codified at N.Y.C. ADMIN. CODE §§ 14-188(j)-(k) and N.Y.C. CHARTER § 803.
[31] *See* N.Y.C. ADMIN. CODE §§ 14-188(a)-(b).
[32] *See* N.Y.C. ADMIN. CODE §§ 14-188(d)-(e).

10. Any potential disparate impacts of the surveillance technology or its use on groups protected under the New York City Human Rights Law.[33]

When surveillance technology is enhanced or put to a use not previously disclosed, the NYPD must publish an addendum to an Impact and Use Policy describing the enhancement or new use.[34]

The 2025 amendments to the POST Act also imposed new requirements on the NYPD specific to the use of facial recognition technology. Some of the requirements of these amendments expand upon the general requirements of the POST Act. For example, with respect to facial recognition technology, the NYPD must not only describe the use restrictions placed on facial recognition but also provide written "procedures for supervisory approval and internal oversight to safeguard against improper use of such technologies."[35] Other aspects are entirely new. For example, the NYPD must have "guidelines related to the modification of the original image used for comparison analysis," and must "conduct an annual audit of its use of facial recognition technology," detailing (1) the total number of comparison requests made by an investigating officer to apply facial recognition technology to a specific image; (2) the total number of instances in which facial recognition technology is applied to a specific image; (3) the total number of instances in which facial recognition technology is applied to an image associated with an investigation for a crime classified as a felony; and (4) the total number of instances in which facial recognition technology is applied to an image associated with an investigation for a misdemeanor.[36] The amendments became effective in September 2025, during the course of this investigation, and mandate that the NYPD complete the audit annually. The NYPD has informed OIG-NYPD it intends to complete the mandated audit each calendar year, beginning in 2026.

As discussed in more detail below, the NYPD has two policy and procedure documents related to the use of facial recognition technology. First, it has its Facial Recognition Impact and Use Policy, which was most recently updated in February 2026 and includes several addenda. Second, it has Patrol Guide § 212-129, titled "Facial Recognition Technology," which has been effective since December 2, 2022, and sets forth the NYPD's internal procedures for the use of facial recognition technology.

The POST Act requires DOI to prepare annual audits of the NYPD's surveillance technology Impact and Use Policies, including: (1) assessment of the NYPD's compliance with the terms of its own policies; (2) descriptions of any known or reasonably suspected violations of the policies; and (3) recommendations on

[33] *See* N.Y.C. ADMIN. CODE § 14-188(a).
[34] *Id.*
[35] N.Y.C. ADMIN. CODE § 14-188(a)(2).
[36] N.Y.C. ADMIN. CODE §§ 14-188.1(b)-(c).

revisions to the Impact and Use Policies.[37] In service of these reports, the POST Act requires the NYPD to make itself available to DOI, including through proactive disclosures of changes to surveillance technologies and the results of annual audits on the use of facial recognition technologies.[38]

## IV. Assessment of the NYPD's Facial Recognition Impact and Use Policy

This report serves to summarize OIG-NYPD's 2025 annual POST Act audit, focusing on the NYPD's Facial Recognition Impact and Use Policy (the "Facial Recognition IUP" or "the Policy"), which was first issued in April 2021, with two subsequent addenda issued October 26, 2023, and November 24, 2023, and revisions made February 4, 2026.[39]

To conduct its audit, OIG-NYPD performed a section-by-section analysis of the most recent version of the Facial Recognition IUP, published in February of this year. OIG-NYPD then compared the Facial Recognition IUP against the NYPD's internal procedures and practices regarding the use of facial recognition technology embodied in a provision of the Department's Patrol Guide, as described during interviews of NYPD officials about the Department's use of facial recognition technology, and as reflected in other information provided by the NYPD. Finally, OIG-NYPD further informed its findings through a review of publicly available news and research articles regarding facial recognition technology, including evaluations of facial recognition algorithms by the National Institute of Standards and Technology ("NIST") and materials discussing the procurement of facial recognition technology by the NYPD.

As noted above, the POST Act requires the NYPD's Impact and Use Policies to address ten topics related to the NYPD's use of any surveillance technology and includes several more requirements specifically related to the use of facial recognition technology. The analysis below tracks each of the topics in the POST Act, first describing how, if at all, the topic is covered in the Facial Recognition IUP, then evaluating whether the NYPD's procedures and practices are consistent with the Facial Recognition IUP, and offering recommendations where the NYPD's procedures or practices are inconsistent with the Facial Recognition IUP or could be improved, or where the Policy lacks information required by the POST Act.

### A. Description of the Capabilities of the NYPD's Facial Recognition Technology

The first requirement set forth in the POST Act for all Impact and Use Policies is that they include "a description of the capabilities of a surveillance technology"[40]

[37] *See* N.Y.C. CHARTER § 803(c-1).
[38] *See* N.Y.C. ADMIN. CODE § 14-188(d); *See also* N.Y.C. ADMIN. CODE § 14-188(1)(c).
[39] The NYPD's Facial Recognition IUP, as updated on February 4, 2026, is attached to this report as Appendix B.
[40] N.Y.C. ADMIN. CODE § 14-188(a).

and "identify the manufacturer and product name of each surveillance technology that is addressed by the impact and use policy, including the specific capability and component of the surveillance technology that is addressed by such policy if such product is listed in more than one such policy."[41]

*The Facial Recognition IUP*[42]: The Facial Recognition IUP explains that facial recognition technologies have been employed at the NYPD since 2011 to "investigate criminal activity and increase public safety" by identifying suspects and persons unable to identify themselves. [43] To do so, the NYPD uses technologies manufactured by Dataworks+ and Idemia.

The Policy explains that NYPD investigators who obtain video or photos over the course of an investigation that contain an image of the face of an unknown individual, can submit the image(s) as a "probe image" for facial recognition analysis.[44] The image(s) are compared to a photo repository consisting of arrest and parole photographs of "individuals that have been charged with a crime where a criminal court has jurisdiction."[45] The repository does not include images associated with sealed arrests, nor the probe images themselves. According to the Policy, the NYPD's facial recognition software then generates a pool of possible match candidates that are to be manually reviewed by trained NYPD facial recognition investigators.

The Policy further states that the NYPD does not perform any real-time facial recognition through its video cameras or systems, nor does it use any other biometric measuring technologies.

The Policy does not identify the product name of each facial recognition technology used by the NYPD.

*The NYPD's Procedures and Practices*: To assess the accuracy of this section of the Facial Recognition IUP, OIG-NYPD interviewed NYPD personnel and reviewed the contract agreements, user manuals, and product inventories of two contractual products that the NYPD uses for facial recognition available from DataWorks+, namely the DataWorks Face Plus program and the PhotoManager System, as well as a third product developed by Idemia Public Security ("Idemia") known as FaceExpert. OIG-NYPD also requested, and received, information from the NYPD to clarify

[41] N.Y.C. ADMIN. CODE § 14-188(b).
[42] The information in this section is derived from Appendix B at 4.
[43] Appendix B at 4.
[44] OIG-NYPD understands facial recognition analysis to be distinct from facial recognition *results*. Facial recognition analysis is conducted solely by certified facial recognition investigators, who make a match determination based on analysis of a pool of candidate photographs produced by software only the facial recognition investigators are authorized to operate. A facial recognition result is the ultimate determination of such analysis. The result is provided to the requesting detective by the facial recognition investigator and includes only the initial probe image and the possible match, if one has been identified, or a no match notification where no possible match has been identified.
[45] Appendix B at 4.

aspects of the NYPD's use of these products that were not evident from those documents.

DataWorks Face Plus is available to the NYPD through a partnership with the Office of National Drug Control Policy's High Intensity Drug Trafficking Areas ("HIDTA") program. The product is manufactured by DataWorks+ and utilizes a biometric matching algorithm to compare probe images to images in a designated photo repository comprised of photographs from arrests made within New York and New Jersey.

A second DataWorks+ product, the PhotoManager System, is available to the NYPD through a direct contract with DataWorks+. The PhotoManager System consists of both a photo repository for facial recognition analysis and the DataWorks+ facial recognition software. The PhotoManager System compares probe images to all NYPD-obtained arrest photos including juvenile arrest photos. Access to the functions of this product that allow for analyses against juvenile photographs is restricted: to conduct an analysis comparing a probe photo to juvenile arrest photos, an investigator must first request access to the juvenile database from the Information Technology Bureau ("ITB"). According to the NYPD, between November 2025 and January 2026, only seven facial recognition searches were run against the database of juvenile arrest photos. The NYPD has informed OIG-NYPD that its contract with DataWorks+ is primarily for the purpose of maintaining the PhotoManager System, which houses its arrest photos, rather than to support facial recognition analysis, except with respect to juvenile arrest photos, which are not included in the photo repositories for the other two facial recognition products used by the NYPD.

Finally, the NYPD has a contract with Idemia for FaceExpert. This product compares probe images against a photo repository of adult arrest photographs from arrests made by the NYPD maintained by Idemia, as it does not interface with the PhotoManager System. While it is functionally similar to the DataWorks Face Plus program, it utilizes a different algorithm to conduct its facial recognition analysis, which can lead to different search results, and is only available to Facial Identification Section ("FIS") personnel.

Based on OIG-NYPD's review of the capabilities of the three facial recognition products in use at the NYPD, the NYPD's Facial Recognition IUP accurately describes the capabilities of its facial recognition technologies. However, there are aspects of the Policy's descriptions that fail to comply with the POST Act or that could otherwise be more accurate.

First, while the Facial Recognition IUP provides "the manufacturer" of its technologies, it does not include the "product name of each surveillance technology," as required by the POST Act.[46] Accordingly, OIG-NYPD recommends as follows:

[46] N.Y.C. ADMIN. CODE § 14-188(b)(3).

> **Recommendation #1:** The NYPD should amend the Facial Recognition Impact and Use Policy to include the names of the three facial recognition products in use at the NYPD.

This amendment will bring the Facial Recognition IUP into compliance with the POST Act's requirement that IUPs reflect "product name[s]."

Second, the Policy's description of the photo repositories utilized for facial recognition analyses, referring to "arrest and parole photographs of individuals that have been charged with a crime where a criminal court has jurisdiction"[47] is inaccurate. OIG-NYPD learned that the NYPD has access to three photo repositories, described above, comprised of different combinations of adult and juvenile arrest photos from New York and New Jersey. Contrary to the IUP and Patrol Guide, and according to the NYPD, none of the photo repositories used by the NYPD for facial recognition analysis contain parole photos. For increased transparency, OIG-NYPD recommends as follows:

> **Recommendation #2:** The NYPD should amend the Facial Recognition Impact and Use Policy to enumerate the photo repositories associated with each of the facial recognition products it uses, as well as to identify specifically from where the photographs contained in the photo repositories are obtained.

This information is readily available to the NYPD and would increase the public's understanding of the NYPD's facial recognition practices.

### B. Uses and Restrictions on the Use of Facial Recognition Technology

The second requirement set forth in the POST Act is that Impact and Use Policies must include:

> [R]ules, processes and guidelines issued by the department regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use, including whether the department obtains a court authorization for such use of a surveillance technology, and, if so, the specific type of court authorization sought.[48]

The POST Act also includes several other requirements specific to the use of facial recognition technologies, which were enacted in September 2025. Specifically, the NYPD must have a policy (whether in the Impact and Use Policy or elsewhere) including:

1. "[A] description of the department's use of facial recognition technologies;"[49]

[47] Appendix B at 4.
[48] N.Y.C. ADMIN. CODE § 14-188(a).
[49] N.Y.C. ADMIN. CODE § 14-188(a)(1).

2. "[R]estrictions placed on access and use of such technologies by department personnel, including procedures for supervisory approval and internal oversight to safeguard against improper use of such technologies;"[50] and

3. "[G]uidelines related to the modification of the original image used for comparison analysis by facial recognition technology," including standards for documenting and maintaining copies of any modified images.[51]

*The Facial Recognition IUP*[52]: The Facial Recognition IUP describes the operational uses of facial recognition technology and the procedures by which facial recognition analysis is requested; it also describes certain special cases, where court authorization or executive-level NYPD approval is required before use.

To begin, the Policy lists six authorized uses of facial recognition technology: (1) identifying an individual when there is a basis to believe that such individual has or will commit a crime; (2) identifying an individual who may be a missing person, crime victim, or witness to criminal activity; (3) identifying a deceased person; (4) identifying a person who is incapacitated or otherwise unable to identify themselves; (5) identifying an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification; and (6) mitigating an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

The Policy then details restrictions on these authorized uses, including that analyses must be used in a manner consistent with the state and federal Constitutions and applicable statutory authority. Finally, the Policy states that facial recognition analyses may only be used to generate investigative leads; they cannot alone establish a basis for a stop, an arrest, or a search warrant.

The Policy includes a detailed procedure for requesting the use of facial recognition technology. If an investigator obtains an image depicting an unidentified individual and intends to use facial recognition technology to help identify the individual, the Policy requires the investigator to make a request for facial recognition analysis and include the case or complaint number for the matter under investigation, along with the probe images to be used. The facial recognition investigator must then confirm that the request is for an authorized use and document that confirmation in "the appropriate NYPD case management system." The Policy then requires the facial recognition investigator to run the facial recognition software to generate a pool of potential match candidates and to manually review the possible match results by performing a human facial comparison. Under the Policy, the "probe images" inputted into the facial recognition software "are only

[50] N.Y.C. ADMIN. CODE § 14-188(a)(2).
[51] N.Y.C. ADMIN. CODE § 14-188(b).
[52] The facts in this section are derived from Appendix B at 5-7.

minimally altered through brightness correction, cropping, or rotating"; they "are never materially altered or enhanced in a manner that affects biometric identifiers."[53] A possible match candidate then undergoes peer review with other facial recognition investigators before a final level of supervisory review.

Where a possible match candidate is not identified, the facial recognition investigator will inform the requesting investigator. Where a possible match is identified, the Policy requires the facial recognition investigator to prepare a "possible match report" for the requesting investigator that includes the probe image, the possible match, and a warning about the evidentiary value of the possible match to the requestor's investigation.

The Policy also describes the limited conditions under which an investigator can seek to use outside facial recognition technologies that compare probe images against photo repositories beyond those discussed above. Under the Policy, use of those technologies is prohibited unless approval is granted by the Chief of Department, the Chief of Detectives, and the Deputy Commissioner of Intelligence and Counterterrorism "for an articulable reason." The same group of individuals are also responsible for deciding whether use of NYPD facial recognition technologies that "ha[ve] not been foreseen or prescribed in policy . . . is appropriate and lawful."

Finally, the Policy includes several provisions addressing other issues. Under the Policy, body-worn camera ("BWC") footage is not routinely submitted for facial recognition, but images derived therefrom may be submitted for authorized purposes. The Policy also prohibits the use of facial recognition to identify and monitor individuals at protests and political rallies, as well as the discriminatory use of such technology. Under the Policy, misuse of facial recognition by NYPD personnel can result in administrative or criminal penalties. The Policy does not require NYPD to seek court authorization for its authorized uses of facial recognition technology.

*The NYPD's Procedures and Practices*: Because this section of the Facial Recognition IUP is the most detailed, OIG-NYPD focused its audit on six areas of inquiry: (1) Who has access to facial recognition technology?; (2) What is the process for conducting facial recognition analysis?; (3) How can "probe images" be modified before use?; (4) How are photo repositories and software products selected for facial recognition analysis?; (5) How are peer reviews conducted?; and (6) How are other use restrictions implemented? Each of these areas of inquiry are discussed below.

### *1. Who Has Access to Facial Recognition Technology?*

Before answering whether the NYPD follows the use procedures for facial recognition technology outlined in the Policy, it is necessary to understand *who* is responsible for use of that technology. The Facial Recognition IUP speaks in general terms, delineating steps that "requesting investigators" and "facial recognition investigators" must take in the facial recognition analysis process.

[53] Appendix B at 6.

Patrol Guide 212-129, titled "Facial Recognition Technology,"[54] contains the internal NYPD procedures that operationalize the NYPD's Facial Recognition IUP and provides more specific information about "facial recognition investigators." Pursuant to the Patrol Guide, in general, requests for facial recognition analysis are submitted to the Real Time Crime Center, Facial Identification Section.[55] According to organizational charts produced by the NYPD to OIG-NYPD, investigators in the Facial Identification Section are part of the Specialty Enforcement Division in the Detective Bureau. Their function, as is the function of other officers assigned to the Real Time Crime Center, is to provide investigative support to detective squads in precincts across New York City.[56] According to logs provided by the NYPD to OIG-NYPD, FIS conducted approximately 26,000 facial recognition analyses in 2025.

Patrol Guide 212-129 also indicates that servicemembers in the Intelligence and Counterterrorism Bureau have access to facial recognition technology. Like investigators in the Facial Identification Section, members of the Intelligence and Counterterrorism Bureau who have authorized access to facial recognition software "must strictly comply with [Patrol Guide 212-129] when utilizing the technology."[57] During this investigation, OIG-NYPD learned through an interview with NYPD personnel that investigators in two units within the Intelligence and Counterterrorism Bureau's Intelligence Division – the Regional Intelligence Support Center ("RISC") and the Special Activities Unit ("SAU") – had authorization to use facial recognition technology from 2019 to 2025. The NYPD verified that RISC processed requests from external entities during this timeframe, while SAU restricted its processing to requests from personnel within the Intelligence and Counterterrorism Bureau.

However, these procedures have since changed. The NYPD informed OIG-NYPD that, effective November 2025, RISC is now the only unit within the Intelligence Division conducting facial recognition analysis, as SAU no longer processes facial recognition requests.

As noted above, the Facial Recognition IUP currently uses a generic reference to "facial recognition investigators." OIG-NYPD recommends as follows:

> **Recommendation #3:** The NYPD should amend its Facial Recognition Impact and Use Policy to specifically identify which Bureaus have access to facial recognition technology, what those Bureaus do, and who they serve.

This will increase transparency by providing the public with an understanding of who within the NYPD is authorized to conduct facial recognition analysis.

---

[54] *See* Appendix C.
[55] *See* Appendix C at 2.
[56] *See Detectives,* NYPD, https://www.nyc.gov/site/nypd/bureaus/investigative/detectives.page (last visited May 19, 2026).
[57] Appendix C at 3-4.

### *2. What Is the Process for Conducting Facial Recognition Analysis?*

Patrol Guide 212-129 outlines a process for the Facial Identification Section to receive requests for, conduct, and document facial recognition analyses consistent with the Policy.

According to the Patrol Guide, a requesting officer is required to document a request to the Facial Identification Section through a computer system called the Enterprise Case Management System ("ECMS") on a form called FIS Request DD5.[58] A FIS investigator assigned to the case must then confirm the basis for the request and document it in the same system.[59] The analysis is then conducted using the same process of probe image selection, software use, manual verification, peer review, and supervisory review that is outlined in the Facial Recognition IUP.[60] If a possible match is found, the FIS investigator sends a FIS Possible Match Report back to the requesting officer, including all the information outlined in the Facial Recognition IUP.[61] The FIS investigator must retain all records of searches, including the case number, reason the search was requested, details, and search results, and upload all of this information into ECMS.[62]

Patrol Guide 212-129 directs Intelligence Division members with access to facial recognition technology to follow the same procedures that FIS investigators follow. However, through interviews with Intelligence Division personnel, OIG-NYPD discovered that – from 2019 to 2025 – the Intelligence Division's practices did not comply with the Patrol Guide. Rather than documenting the facial recognition analysis process through ECMS, Intelligence Division personnel who conducted facial recognition analysis received requests and distributed facial recognition results by email.

Monitoring facial recognition requests through two separate systems, ECMS and email, was not only inconsistent with the Patrol Guide, but also increased the risk that (1) requests for, and results of, analyses would not be properly documented or preserved in an easily accessible system; and (2) multiple units would assist on the same case through the unnecessary, repeated use of facial recognition technology with inconsistent results. This latter risk is exactly what Legal Aid alleges occurred in one instance highlighted in its referral, where Legal Aid wrote:

> [A] detective sent a surveillance video to FIS in order to identify a suspect in [a] video. FIS determined that there was no match found for the unidentified suspect. The investigating detective's DD5 [worksheet] states that she was advised of an FIS no match notification. But just a

[58] *Id.* at 2.
[59] *Id.*
[60] *Id.* at 2-3.
[61] *Id.* at 3.
[62] *Id.*

> few hours later, there was another DD5 [worksheet] from the same detective stating that she was uploading a possible FIS match. A review of ECMS records clearly shows that possible match came from SAU, not FIS.[63]

OIG-NYPD could not independently corroborate Legal Aid's allegations because it could not access records associated with the underlying sealed arrest.[64] RISC and SAU facial recognition investigators confirmed that they did not actively collaborate with FIS on their facial recognition analyses. The policies and practices employed by the Intelligence Division through 2025 created a risk that investigators across multiple units may have independently analyzed the same case without awareness of each other's efforts and produced different results.

FIS and Intelligence Division investigators also documented the results of their analyses in different ways. The Facial Identification Section followed procedures broadly consistent with the Facial Recognition IUP. FIS investigators log analysis results in ECMS. Sample ECMS records reviewed by OIG-NYPD reflect that analyses with negative results are logged with a statement of the results. Where a possible match is found, certain information is logged such as the FIS case number, the FIS investigator's name, the crime alleged to have been committed, the requesting detective's name, command, and detective case number, as well as "possible lead information" such as the name, New York State Identification Number, and the date of arrest associated with the possible match image.

By contrast, the Intelligence Division logged their results in a paper log from 2019 to 2023, and a digital log from 2024 to 2025. The latter provided information like the case number, the requestor, the facial recognition investigator ("recorder"), whether a match was made, and whether a supervisor reviewed the match. The Intelligence Division's documentation process had readily apparent errors. For example, OIG-NYPD reviewed the digital logs and found that 33% of log entries listed a single facial recognition investigator as both the requestor and the recorder, despite the fact that facial recognition investigators did not carry their own caseloads. Moreover, the Intelligence Division's approach did not comply with the Patrol Guide, which requires "search results" to be "upload[ed] [] into the ECMS case file."[65]

Fundamentally, the inconsistent documentation practices between the Intelligence Division and FIS made it difficult to (1) track the results of facial recognition analyses across the different units; (2) ensure that multiple units were

[63] Appendix A.

[64] OIG-NYPD contacted the Legal Aid Society, which subsequently directed the Office to a private civil attorney who had represented the individual identified as a possible match. OIG-NYPD's attempts to speak with the individual's attorney were unsuccessful. As a result, OIG-NYPD was unable to review the individual's records and the DD5 worksheets in question. Nonetheless, as indicated herein, OIG-NYPD confirmed that NYPD practices in effect through 2025 allowed for the type of situation identified by Legal Aid in its letter to occur. As described below, those practices have since changed.

[65] Appendix C at 3.

not conducting facial recognition analysis on the same case, and (3) ensure investigators were complying with the Policy.

The NYPD informed OIG-NYPD that, as of January 2026, RISC no longer uses email to process facial recognition requests. Instead, RISC – the only Intelligence Division unit currently authorized to conduct facial recognition analysis – processes all facial recognition matters through the Intelligence Division Case Management System ("IDCMS"). According to the NYPD, IDCMS is a system similar to the ECMS system utilized by FIS. When RISC receives a request from an internal or external entity for facial recognition analysis, RISC personnel create a folder in IDCMS and save the corresponding DD5 (indicating an image rejection, no match, or possible match) within IDCMS. For requests from external entities, the response is also sent via email to the external entity. RISC also processes facial recognition requests for Field Intelligence Officers ("FIOs") deployed to each precinct. Because FIOs have access to ECMS, which interfaces with IDCMS, an FIO can submit a request by completing the appropriate DD5 in ECMS, automatically creating a case in IDCMS. The RISC investigator then completes the facial recognition analysis, enters the appropriate response DD5, and transmits it back to the FIO from IDCMS to ECMS.

The NYPD further informed OIG-NYPD that, as of late August 2025, an investigator assigned to the Detective Bureau can only request a facial recognition analysis from FIS[66] and, as of late November 2025, an investigator assigned to the Intelligence and Counterterrorism Bureau can only request a facial recognition analysis from RISC, as SAU no longer processes facial recognition requests.[67]As of this writing, the Patrol Guide has not been updated to reflect any of these changes.

To ensure standard practices across the NYPD and that the Patrol Guide reflects current NYPD practices, OIG-NYPD issues the following recommendations:

> **Recommendation #4:** The NYPD should update Patrol Guide 212-129 to instruct personnel to request facial recognition analysis only from the authorized unit within their assigned Bureau.

[66] The NYPD provided OIG-NYPD with an email dated August 20, 2025, which documents this change and indicates that facial recognition requests "for cases investigated by the Detective Bureau" would no longer be submitted "to SAU or the RISC" and indicating to recipients that this information was "[f]or your immediate compliance." Notably, however, OIG-NYPD's review of the Intelligence Division's FRT logs show that Detective Bureau personnel made multiple requests for facial recognition analysis by the Intelligence Division through October 2025, indicating that implementation of this change was not immediate.

[67] The NYPD provided OIG-NYPD with an email dated November 18, 2025 from an SAU Lieutenant to an "All Users – SAU" mailing list documenting this change. The email states that "[e]ffective [i]mmediately SAU will no longer be conducting Facial Recognition Requests[.] The RISC will be handing all Facial Rec Requests moving forward." Notably, however, in December 2025, OIG-NYPD interviewed an SAU detective who had previously been authorized to conduct facial recognition analysis, who did not alert OIG-NYPD to this recent change, suggesting that practical implementation of the change may not have been immediate.

> **Recommendation #5:** The NYPD should ensure that facial recognition analysis logs in both the Enterprise Case Management System and the Intelligence Division Case Management System are standardized to capture consistent and accurate data collection across all entries.

Standardizing the documentation and transmittal of information across the Intelligence and Counterterrorism Bureau and the Detective Bureau, and updating the Patrol Guide to reflect current practice, ensures that the NYPD is in compliance with the Patrol Guide, allows for appropriate auditing, and eliminates the risk of duplicative and inconsistent analyses, as alleged by the Legal Aid Society in its 2025 letter to this Office.[68]

*3. Can "Probe Images" Be Modified Before Use?*

The Facial Recognition IUP, as published in February 2026, provides that probe images "are only minimally adjusted through brightness correction, cropping, or rotating for clarity purposes" and, "are never materially altered or enhanced in a manner that affects biometric identifiers."[69] Prior versions of the Facial Recognition IUP, including addenda to the Policy, in effect from December 2022 until February 2026 did not include these provisions. This indicates that material alterations and enhancements affecting biometric identifiers were not specifically prohibited prior to February 2026 and therefore also suggests that such enhancements previously occurred, which OIG-NYPD's audit has substantiated, as described below.

Enhancement of probe images is acknowledged to be a feature incorporated into many facial recognition technologies.[70] The facial recognition software utilized by the NYPD includes standard features to improve image clarity, such as brightness correction, contrast, and sharpness. However, OIG-NYPD's review of the FaceExpert and PhotoManager user manuals revealed that both software programs include features that permit probe image editing beyond what the NYPD's current policy allows. For instance, one software features a "paint brush" tool that enables users to "paint onto the image", potentially altering biometric identifiers. The other software includes a feature enabling users to export the probe image into an external photo editing application before uploading it for analysis. During interviews, NYPD personnel confirmed that, while SAU and RISC did not use these enhancement techniques, several years ago certain FIS investigators who are no longer with the Department did utilize them. Use of such now-prohibited features may have

[68] Appendix A at 2.
[69] Appendix B at 6.
[70] *See* Maria Eira, et al., *A Policy Framework for Responsible Limits on Facial Recognition, Use Case: Law Enforcement Investigations,* WORLD ECON. F., (Nov. 2022), page 25, https://www.weforum.org/publications/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case- law enforcement-investigations-revised-2022/ (last visited Feb. 26, 2026); *See also* Clare Garvie, *Garbage In, Garbage Out Flawed Face Data,* GEO. L. CTR. ON PRIV. & TECHN., (May 16, 2019), https://www.flawedfacedata.com/ (last visited Oct. 31, 2025) ("Editing photos before submitting them for search is common practice, as suggested by responses to records requests and a review of the software packages that face recognition vendor companies offer.").

increased the likelihood of a possible match result following FIS analysis conducted by these since-departed FIS investigators, as compared to analysis conducted by SAU or RISC.

The NYPD disclosed to OIG-NYPD that, prior to 2023, NYPD personnel utilized probe image enhancement techniques that were subsequently prohibited in the Policy adopted in February 2026. Indeed, as part of this investigation, the NYPD produced a 2024 PowerPoint presentation developed by FIS as part of the NYPD's Criminal Investigation Course ("CIC") designed to teach detectives about the capabilities of the Facial Identification Section and to be made available to outside law enforcement agencies to show the unit's capabilities, which confirms the NYPD's prior use of now-prohibited enhancements. The presentation included examples demonstrating the use of enhancement tools to improve the likelihood of matching probe images when key physical features in the source image are obstructed – such as by a COVID-19 face mask – or are otherwise insufficient for comparison. The presentation also included examples for the use of enhancement tools in cases where individuals were incapacitated and unable to identify themselves, as well as postmortem identification scenarios. Finally, the presentation also discussed scenarios when investigators substituted publicly available photographs of high-profile individuals for facial recognition analysis in lieu of submitted probe images, in violation of the Policy.[71] The NYPD has informed OIG-NYPD that these enhancement techniques were never common practice and that their use ceased entirely in 2022.[72] The NYPD further clarified that, while the presentation indicated a date of 2024, it was last presented to CIC attendees in 2022. According to the NYPD, although the presentation was not used after 2022, a copy of the presentation was retained, periodically updated (including in 2024), renamed accordingly, and kept available for future use.

While the NYPD's limited use of such techniques apparently ceased in 2022, OIG-NYPD's review of all policies, procedures, guidelines, operation orders, and internal memoranda regarding the use of facial recognition technology provided by the NYPD did not reveal any materials from 2022 or thereafter specifically instructing facial recognition investigators not to use such enhancement techniques. Furthermore, Patrol Guide 212-129, last published in December 2022, contains no image enhancement guidelines.

---

[71] *See* John Schuppe, *NYPD Used Celebrity Doppelgangers to Fudge Facial Recognition Results, Research's Say,* NBC News, (May 16, 2019), https://www.nbcnews.com/news/us-news/nypd-used-celebrity-doppelg-ngers-fudge-facial-recognition-results-researchers-n1006411 (last visited May 20, 2026); Appendix B at 4-5 ("If a video or photo contains an image of a face of an unknown individual, the image can be submitted for facial recognition analysis in accordance with NYPD Facial Recognition IUP.") ("Specifically, the request is made for the image depicting the face of the unknown person (the probe image) to be compared to photos in the arrest and parole photo repository.").

[72] The slides in the presentation that demonstrate celebrity enhancement techniques are attributed to two detectives who, according to the NYPD, are no longer with the Department.

To ensure compliance with the Facial Recognition IUP's standards for image modification and to comply with the 2025 POST Act amendments, OIG-NYPD recommends the following:

> **Recommendation #6:** The NYPD should update Patrol Guide 212-129 to memorialize the Facial Recognition Impact and Use Policy's guidelines regarding acceptable image enhancement techniques.
>
> **Recommendation #7:** The NYPD should establish and document an authorization process requiring facial recognition investigators to obtain permission from the Chief of Detectives or Chief of Intelligence (depending on the relevant Bureau the facial recognition investigator is assigned to) prior to editing probe images beyond standard parameters.
>
> **Recommendation #8:** The NYPD should implement a mandatory documentation process to log all probe image modifications in compliance with the 2025 POST Act amendments.

These recommendations are necessary for the NYPD to comply with the POST Act, will improve the transparency of the NYPD's facial recognition practices, and ensure that the NYPD's practices can be properly audited.

*4. How are Photo Repositories and Software Products Selected for Facial Recognition Analysis?*

As discussed above in the "capabilities" section, the NYPD utilizes three different FRT software programs. However, the Facial Recognition IUP's "use" section and Patrol Guide 212-129 provide no guidance regarding the circumstances under which each of the three programs should be used. The NYPD further confirmed that there is no additional guidance provided to facial recognition investigators on how to select the appropriate software and corresponding photo repository.

To ensure consistent results in the NYPD's application of facial recognition technologies, OIG-NYPD recommends as follows:

> **Recommendation #9:** The NYPD should amend the Facial Recognition Impact and Use Policy and Patrol Guide 212-129 to include guidance on how to select which facial recognition software program to use when conducting facial recognition analyses.

Standardizing this process will help ensure that cases are treated alike and will reduce the need for multiple facial recognition analyses on the same subjects.

According to the Facial Recognition IUP, the NYPD may also utilize outside facial recognition technologies with larger photo repositories if approval is granted "in a specific case, for an articulable reason, by the Chief of Department, Chief of Detectives, *and* Deputy Commissioner of Intelligence and Counterterrorism."[73] The

[73] Appendix B at 7.

Patrol Guide uses similar language, but states that approval may be given "by the Chief of Detectives, Intelligence and Counterterrorism Bureau, *or* Chief of Intelligence."[74] This discrepancy, both in the list of approving officials and the use of the additive "and" in the Facial Recognition IUP and the disjunctive "or" in the Patrol Guide, creates a misleading impression about the rigor involved in obtaining approval to use external photo repositories in practice.

To better understand the NYPD's practices on requesting facial recognition analysis from other entities, OIG-NYPD requested all records from 2019 to November 2025 related to requests to access outside facial recognition photo repositories by members of the NYPD. The NYPD produced logs reflecting 98 approvals between October 2023 and October 2025. The NYPD did not log such requests prior to October 2023 and did not provide logs for any denied requests. According to the logs provided, each approved request was made by members of the Intelligence and Counterterrorism Bureau, approved by the Assistant Commissioner for Intelligence and Counterterrorism, and sent to United States Customs and Border Protection for analysis. Approval by this Assistant Commissioner was not consistent with the version of the Facial Recognition IUP in effect during that time period.[75] Moreover, the logs produced by the NYPD were sparse; for example, they did not include information detailing the reasons requests were granted[76] or showing which requests – if any – were denied.

To improve the consistency of the NYPD's practices regarding the use of outside facial recognition technologies, OIG-NYPD recommends the following

> **Recommendation #10**: The NYPD should amend the Facial Recognition Impact and Use Policy, Patrol Guide 212-129, and other related policies to (1) clearly indicate which individual(s) in the Intelligence and Counterterrorism Bureau are authorized to review facial recognition analysis requests to outside agencies; and (2) require formal documentation of the outside request process in both the Detective Bureau and the Intelligence and Counterterrorism Bureau, including whether each request was approved or denied along with the reasoning behind the decision.

Elaborating upon the Policy on outside requests will help ensure that NYPD officials employ consistent standards for determining whether an investigator has presented an "articulable reason" for a request, standardize the supervisory approval structure, and improve documentation needed for meaningful oversight of the NYPD's use of facial recognition technology.

---

[74] Appendix C at 3-4.

[75] The same officials were authorized to approve these requests during that period. However, the Facial Recognition IUP used "or" rather than "and" prior to 2026, showing that any one official could approve a request.

[76] The records did indicate the type of case under investigation. For example, 36% of requests were for cases regarding individuals "supportive of foreign terrorist organization."

### *5. How are Peer and Supervisor Reviews Conducted?*

Peer and supervisory review are part of the facial recognition analysis process in both the Facial Recognition IUP and the Patrol Guide. After an initial possible match is made, the Facial Recognition IUP states that the possible match "is submitted for peer review to other facial recognition investigators,"[77] as does the Patrol Guide.[78] Thereafter, "[a] supervisor of the facial recognition investigator performs a final review of a possible match candidate and provides final approval, if appropriate."[79] Presentations given by FIS also confirm that peer review is a mandatory step in the facial recognition workflow.

OIG-NYPD identified three issues in the implementation of the peer and supervisory review process at the NYPD. First, the Intelligence Division does not appear to consistently track or conduct supervisory review. The Intelligence Division produced two internal logs documenting facial recognition analysis, as discussed on page 16. The first log, documenting analyses conducted from 2019 to 2023, lacked a supervisory review column, preventing OIG-NYPD from verifying whether such reviews occurred. In the second log, documenting analyses from 2024 to 2025, OIG-NYPD found that approximately 33% of facial recognition searches were marked "no" for supervisor review. Though arguably ambiguous (see footnote 79), the most sensible reading of both the IUP and the Patrol Guide requires supervisory review of all possible matches. Indeed, the NYPD has indicated to OIG-NYPD that it understands the language in the Patrol Guide to require such supervisory review. Second, while research (including research published by the manufacturer of one of the NYPD's facial recognition products) suggests that "blind" peer review should be followed in facial recognition analyses,[80] the NYPD's policies contain no guidance on *how* to conduct peer review. Blind peer review allows the reviewer's assessment to remain a product of his or her own expertise and uncompromised judgment. This

---

[77] Appendix B at 6.
[78] *See* Appendix C at 3.
[79] Appendix B at 6; *see also* Appendix B at 3 ("Conduct final review of possible match candidate, and approve, if appropriate."). The language in both the Facial Recognition IUP and the Patrol Guide is arguably ambiguous as to whether supervisory review is mandatory. Both documents refer to supervisory review and approval "if appropriate." As a result, it is possible to read the documents to say that a supervisor only needs to review "if appropriate," though the significantly more sensible reading is that the supervisor should only approve a match "if appropriate" following a mandatory supervisory review, given that neither the IUP or the Patrol Guide provide information regarding how to assess whether supervisor review is appropriate. As indicated above, the NYPD has also stated that the Patrol Guide requires supervisory review for any possible match.
[80] *See* Maria Eira, et al., *A Policy Framework for Responsible Limits on Facial Recognition, Use Case: Law Enforcement Investigations,* WORLD ECON. F., (Nov. 2022), page 26, *at* https://www.weforum.org/publications/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case- law enforcement-investigations-revised-2022/ (last visited Feb. 26, 2026); *See also Use of Facial Recognition Technology for Law Enforcement Investigations,* IDEMIA PUB. SEC., 5 (Apr. 17, 2025), *at* https://www.idemia.com/wp-content/uploads/2025/04/position-paper-facial-recognition-technology- law enforcement-investigations-idemia-17042025.pdf (last visited Dec. 8, 2025).

decreases the potential for bias in the reviewer's assessments and protects the integrity of the investigative work. Third, none of the units authorized to conduct facial recognition analyses document the occurrence or results of peer review, and only the Intelligence Division documented the occurrence of supervisory review, limiting the ability to audit whether those reviews are, in fact, occurring and the outcomes of any such reviews.

To improve the clarity and transparency of the NYPD's peer and supervisory review processes, OIG-NYPD recommends as follows:

> **Recommendation #11:** The NYPD should amend the Facial Recognition Impact and Use Policy and all associated policies to require mandatory supervisory review and blind peer review for all facial recognition analyses, and to mandate the documentation of reviewer names and result outcomes.

This clarification will help ensure consistent application of the NYPD's review process and will promote effective oversight through the generation of relevant records that can be audited.

*6. How are Other Use Restrictions Implemented?*

The principal use restrictions provided in the Facial Recognition IUP prohibit the NYPD's use of facial recognition in two scenarios: (1) the real-time use of body-worn cameras; and (2) the monitoring and identification of individuals at protests and in political rallies.[81] OIG-NYPD's review of all facial recognition technology used by the NYPD confirms that such technology does not allow for real time analysis, including real time analysis from an officer's body worn camera. In interviews, facial recognition investigators at FIS, SAU, and RISC all confirmed that they do not and have not performed real-time facial recognition analyses.

Regarding the monitoring and identification of individuals at protests and political rallies, the NYPD explained that each request for facial recognition analysis must include an underlying criminal offense and case number. Because analysis is restricted to active criminal investigations, any facial recognition requests connected to protests or political demonstrations are permissible only when they directly relate to a criminal offense.

[81] Due to the limited scope of this report and time constraints, OIG-NYPD did not review each facial recognition analysis to audit the accuracy of requesting officers' statements that facial recognition analyses had been requested for one of the six authorized purposes, nor whether officers followed the restriction that facial recognition analyses not be used to establish probable cause alone. The NYPD, however, produced templates for "Possible Match," "No Match" and "Rejected Sample" reports and each report template clearly states that the analysis outcome does not constitute probable cause to arrest. Each report also clearly requires the listing of a crime and complaint number associated with the attached probe image.

### C. The Prevention of Unauthorized Access

The third requirement in the POST Act is that Impact and Use Policies must include the "safeguards or security measures" taken by the NYPD "designed to protect information collected by [a] surveillance technology from unauthorized access, including but not limited to the existence of encryption and access control mechanisms."[82]

*The Facial Recognition IUP*[83]: The Facial Recognition IUP details internal NYPD access controls related to both the operation of facial recognition technologies and access to the results of facial recognition analyses.

Operation of the technologies is limited solely to NYPD investigators who have an assignment that requires use of facial recognition and who subsequently receive the required facial recognition training and certification. This includes FIS facial recognition investigators whose assignment exclusively constitutes facial recognition analysis, and Intelligence Division personnel whose assignments include – but do not exclusively consist of – facial recognition analysis. Facial recognition investigators' access is conditioned on authentication by username and password and on the successful completion of mandatory training related to the use of the technology.

The results of facial recognition analysis are only provided to detectives who have requested such analysis with an "articulable need to access the system in furtherance of lawful duty." Rights to view facial recognition results are again conditioned on authentication by username and password and the NYPD authorizes access to systems based only on need, according to role.

More broadly, NYPD computer systems are protected by an enterprise architecture program that provides access to systems on a case-by-case basis. Passwords are never stored locally and all data on NYPD computer systems is encrypted both in transit and at rest, following what the NYPD describes as best practices. NYPD personnel are responsible for complying with security terms and conditions respecting their computers and the NYPD case management system and are further responsible for ensuring lack of unauthorized access to third parties by following NYPD's confidentiality rules. These responsibilities are enforced through administrative and potentially criminal penalties.

*The NYPD's Procedures and Practices*: Prior to November 2025, the NYPD provided OIG-NYPD with a list of personnel approved to access and operate facial recognition technology, and all the approved personnel were within FIS, SAU, or RISC.[84] The Office is not aware of any instances in which an individual or entity not authorized to conduct facial recognition analysis has been given access to the NYPD's

[82] N.Y.C. ADMIN. CODE § 14-188(a).
[83] The information in this section is taken from Appendix B at 7-8.
[84] As discussed above, effective November 2025, the NYPD informed OIG-NYPD that RISC is now the only unit within the Intelligence Division conducting facial recognition analysis, as SAU no longer processes facial recognition requests.

facial recognition technologies. Neither the Policy nor the Patrol Guide prohibit detectives who receive facial recognition results from facial recognition investigators from sharing those results with colleagues or supervisors to further their investigation.

### D. The Retention, Access, and Use of Data

Next, the POST Act requires Impact and Use Policies to document "policies and/or practices relating to the retention, access, and use of data collected by [a] surveillance technology."[85] In addition, the 2025 amendments to the POST Act require that the NYPD develop a policy for facial recognition technology that includes "data retention and use policies, including policies applicable to department personnel utilizing [] searches through third-party platforms."[86]

*The Facial Recognition IUP*[87]: The Facial Recognition IUP limits the results of facial recognition analyses to individuals with a legitimate law enforcement purpose, who access the records through the NYPD's computer or case management systems after authentication with a username and password. As noted above, access is limited to individuals with an "articulable need" for an analysis.

NYPD record retention is governed by a schedule derived from the City Charter, approved by both the Law Department and the Department of Records and Information Services. The length of record retention depends on the classification of a record and the final disposition of a case. Records are not disposed of until an investigation and prosecution have been fully exhausted, including any appeals, depending on the way the case progressed.

*The NYPD's Practices and Procedures*: As discussed above, the Facial Identification Section stores records in accordance with the Facial Recognition IUP by uploading the results of facial recognition analyses on ECMS. Before 2026, Intelligence Division investigators' practices deviated from the IUP, as they conveyed analysis results by email and documented their analyses in a log outside of ECMS. In 2026, the Intelligence Division began using IDCMS to process requests for facial recognition analysis and store analysis results.

Regarding access, access to the Data Works Face Plus program is granted through a partnership with HIDTA that operates the program. Access to the NYPD's Idemia program and PhotoManager System is granted by the NYPD's Information Technology Bureau. According to the NYPD, ten FIS investigators, fifteen Special Activities Unit investigators, and eight Regional Intelligence Support Center investigators had access to facial recognition technology at various times between 2019 and 2025. Access was granted to each of these individuals after they completed a four-day training module offered by the FBI.

[85] N.Y.C. ADMIN. CODE § 14-188(a).
[86] N.Y.C. ADMIN. CODE § 14-188(a)(3).
[87] The information in this section is taken from Appendix B at 8-9.

During its review, the Office did not audit: (1) whether any NYPD officers accessed facial recognition results without "articulable need"; (2) whether the NYPD has uniformly followed its retention policies with respect to facial recognition analyses; or (3) whether the NYPD follows its stated retention and use policy for facial recognition analyses conducted through third-party platforms. Given the recent 2025 amendments to the POST Act requiring such policies for analyses conducted by third parties, the NYPD should ensure that the Facial Recognition IUP (or another NYPD policy) adequately addresses these third-party analyses. Consequently, OIG-NYPD recommends the following:

> **Recommendation #12:** The NYPD should update the Facial Recognition Impact and Use Policy and related policies to codify procedures for facial recognition requests performed by outside entities, establish guidelines for officers' use of the results, and ensure that this process is documented and auditable.

This update would bring NYPD into compliance with the 2025 amendments to the POST Act, address the concern regarding use of third-party analyses raised by Legal Aid in its 2025 letter to this Office,[88] and enable OIG-NYPD to conduct audits of this process in a consistent and expeditious manner.

### E. The Use of Data by Members of the Public

The fifth requirement of the POST Act is that Impact and Use Policies include "policies and procedures relating to access or use of the data collected through [a] surveillance technology by members of the public."[89]

*The Facial Recognition IUP*[90]: The Facial Recognition IUP states in full: "Members of the public may request information obtained from the NYPD's use of facial recognition technology pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of the law and NYPD policy."

*The NYPD's Practices and Procedures*: OIG-NYPD conducted a review of publicly available information to determine whether the NYPD made records available to the public through the Freedom of Information Law ("FOIL"). OIG-NYPD found at least two lawsuits related to access to facial recognition records from the NYPD: one filed by the Legal Aid Society in 2020 and another filed by Amnesty

[88] See Appendix A at 2. The incident discussed in the Legal Aid Society's letter involved an NYPD officer's use of a facial recognition analysis conducted by a Fire Department official. The incident was discussed in a judicial opinion dismissing the indictment of the individual who was arrested following a facial recognition match forwarded by the Fire Department to the NYPD. In that opinion, the court concluded that the facial recognition analysis conducted "clearly contravene[d] official NYPD policy concerning the use of facial recognition" because "FDNY's facial recognition software crawled the web" for potential matches and "the NYPD does not permit a facial recognition search to extend as widely as it did." *People v. Zuhdi A.*, 86 Misc. 3d 1227(A) (N.Y. Sup. Ct. 2025).

[89] N.Y.C. ADMIN. CODE § 14-188(a).

[90] The information in this section is taken from Appendix B at 9.

International USA in 2020.[91] The NYPD released certain records related to facial recognition in response to the FOIL requests underlying both lawsuits, confirming that the NYPD provides some facial recognition records in response to FOIL requests, as contemplated in the Facial Recognition IUP (even though in both cases, the *scope* of disclosures resulted in legal disputes).

### F. Disclosure to Outside Entities

The sixth requirement of the POST ACT is that Impact and Use Policies include the "names of all entities outside the department, including local government entities, state government entities, federal government entities, or private entities, that have access to the information and data collected by such surveillance technology."[92] The information must include: "(a) the type of information and data that may be disclosed to each such entity, and (b) the specific safeguards or restrictions imposed by the department on each such entity regarding the use or dissemination of the information and data collected by such surveillance technology."[93]

*The Facial Recognition IUP*[94]: The Facial Recognition IUP explains that no outside entities have direct access to the information derived from the NYPD's facial recognition technology, nor does the NYPD have any agreement with external entities to run facial recognition analyses on their behalf. However, the Policy discusses three categories of entities that may nevertheless receive data from the NYPD related to facial recognition analyses: (1) outside law enforcement agencies; (2) community groups, civil organizations, and the media; and (3) vendors and contractors.

- **Law Enforcement:** Outside law enforcement agencies may request that the NYPD run a facial recognition analysis and the NYPD will honor the request if it accords with the NYPD's procedures for running such analysis. Outside law enforcement agencies may also request pre-existing facial recognition analyses from the NYPD consistent with local law and NYPD policies. Finally, the NYPD is required to disclose the results of facial recognition analyses that relate to criminal cases in accordance with criminal discovery laws.
- **Community Groups and Media:** In accordance with state and local law, the NYPD may provide information to community leaders,

[91] *See Legal Aid Soc'y v. Recs. Access Officer,* 238 A.D.3d 17 (N.Y. App. Div. 2025); *See also Amnesty Intern. USA v. New York City Police Dept.,* No. 156672/2021, 2023 WL 158777 (N.Y. Sup. Ct. Jan. 09, 2023); *See also* Xitai Wang, *Rights groups claim 2,700 NYPD documents disclosed in lawsuit reveal 'surveillance abuses',* JURIS NEWS (Nov. 14, 2025), *at* https://www.jurist.org/news/2025/11/rights-groups-claims-2700-nypd-documents-disclosed-from-lawsuit-reveal-surveillance-abuses (last visited Feb. 26, 2026).

[92] N.Y.C. ADMIN. CODE § 14-188(a).

[93] *Id.*

[94] Information in this section is taken from Appendix B at 9-10.

civic organizations, and the media to further investigations, create awareness, or address community concerns.

- **Vendors and Contractors:** Both facial recognition technology vendors and other NYPD contractors may also access facial recognition data. For contractors, the NYPD "follows the principle of least privilege," providing contractors with information "on a 'need to know basis' to fulfill contract obligations and/or agreements." All vendors and contractors undergo vendor responsibility determinations and integrity reviews and are legally obligated to ensure the confidentiality of NYPD data. Some also undergo background checks.

To the extent any potential external disclosures involve identifying information, the NYPD makes the disclosure only if one of seven enumerated privacy requirements apply. NYPD reports to the Chief Privacy Officer on a quarterly basis detailing any disclosures or collections made in violation of the Identifying Information Law, and the Chief Privacy Officer, in turn, consolidates this information and generates a comprehensive report.

*The NYPD's Practices and Procedures*: OIG-NYPD focused its audit on two categories of outside entities: outside law enforcement agencies and the vendors who provide the NYPD with facial recognition technologies.

With respect to outside law enforcement agencies, the Patrol Guide states that all members of the Detective Bureau "should direct all requests from outside agencies to the Facial Identification Section on an FIS Outside Agency form."[95] It further provides that "[m]embers of the Intelligence Division who have authorized access to facial recognition software must strictly comply with" the same provision of the Patrol Guide.[96] NYPD officials informed OIG-NYPD that this language permits the Intelligence Division to independently process outside agency requests, a practice investigators confirmed during interviews. However, the Patrol Guide does not address the fact that the Intelligence Division uses a different database (IDCMS) than FIS (ECMS) to document its facial recognition requests, nor whether FIS and the Intelligence Division have access to the information necessary to determine whether the other has already responded to an external request. This lack of clarity creates a risk of duplicative facial recognition analyses by the Intelligence Division and FIS. Accordingly, the Office recommends as follows:

> **Recommendation #13:** The NYPD should adopt procedures in Patrol Guide 212-129 sufficient to ensure that FIS and the Intelligence Division do not process the same outside facial recognition requests.

[95] Appendix C at 3-4.
[96] *Id*.

This recommendation can be implemented by different means. For example, the NYPD could simply choose to route all outside facial recognition requests to one Bureau. Alternatively, the NYPD could adopt procedures to allow FIS and the Intelligence Division to cross-reference one another's documentation to ensure that duplicative searches are not being run. OIG-NYPD defers to the NYPD on how best to implement this recommendation.

With respect to vendors, OIG-NYPD confirmed that both DataWorks+ and Idemia have access to the data associated with their related products. The Office also confirmed that those entities are subject to vendor responsibility determinations, integrity reviews, and background checks. They are also obligated by contract to maintain the confidentiality of all NYPD data and information, consistent with the requirements described in the Facial Recognition IUP.

### G. The Training of Facial Recognition Investigators

Next, the POST Act requires that Impact and Use Policies disclose "whether any training is required by the department for an individual to use [a] surveillance technology or access information collected by [a] surveillance technology."[97]

*The Facial Recognition IUP*[98]: The Facial Recognition IUP reads, in full: "NYPD personnel utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, and the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training."

*The NYPD's Practices and Procedures*: The only mandated training that NYPD personnel authorized to use facial recognition technology undergo is a four-day training offered by the FBI. In interviews, facial recognition investigators informed the Office that the FBI's training focused largely on image comparison principles. As described by the NYPD, the FBI training did not provide any instruction on the "operation of the technology." That is to say, the FBI did not train investigators on how to use DataWorks+ and Idemia software. According to the NYPD, DataWorks+ and Idemia provided a one-time training for their products at the time that the NYPD signed contracts with each of these vendors. As a result, if an investigator joined either FIS or the Intelligence Division after the signing of these contracts, they did not receive any formal training on the use of the products.

As a result, OIG-NYPD recommends as follows:

> **Recommendation #14:** The NYPD should provide training on the operation of facial recognition technology and related NYPD policies regarding the use of such technology to all investigators authorized to conduct searches.

[97] N.Y.C. ADMIN. CODE § 14-188(a).
[98] The information in this section is taken from Appendix B at 10.

Training all authorized investigators on the operation of facial recognition technology will ensure that the NYPD complies with its own stated standard – specifically, that personnel receive instruction on the "proper operation of the technology and equipment" in addition to the FBI's existing training on image comparison principles. In addition, providing training on NYPD policies regarding the use of such technology will assist in ensuring compliance with NYPD policies, including recent changes to such policies.

Moreover, the field of facial recognition technology is rapidly evolving.[99] The NYPD's current training program, requiring only one training in advance of becoming a facial recognition investigator in the first instance, risks that the proficiency of its investigators will fall behind improvements in technology. Accordingly, OIG-NYPD recommends as follows:

> **Recommendation #15:** The NYPD should establish recertification requirements involving additional training at periodic intervals for its facial recognition investigators.

Recertification will allow the NYPD's facial recognition investigators to remain apprised of the latest information available on the technology they use.

### H. Internal Audit and Oversight Mechanisms

The seventh requirement set forth in the POST Act is that Impact and Use Policies must include a "description of internal audit and oversight mechanisms within the department to ensure compliance with the surveillance technology impact and use policy governing the use of such surveillance technology."[100] The 2025 amendments to the POST Act mandate "an annual audit of [the NYPD's] use of facial recognition policy," that includes aggregate data on: (1) the number of comparison requests made for a specific image; (2) the number of instances that facial recognition analysis is applied to a specific image; (3) the total number of facial recognition analyses related to felonies, disaggregated by crime; and (4) the total number of facial recognition analyses related to misdemeanors.[101]

*The Facial Recognition IUP*[102]: The Facial Recognition IUP vests NYPD supervisors with responsibility to ensure that facial recognition is used according to policy, including by conducting inspections at least once per tour to make sure computer systems are being used appropriately. Moreover, the misuse of computer systems may result in administrative and potentially criminal penalties, with the

[99] *See* Appendix B, page 11, "over the last half decade, NIST has identified major improvements in the accuracy of facial recognition software"; *See also* Beibut Amirgaliyev et al., *A Review of Machine Learning and Deep Learning Methods for Person Detection, Tracking and Identification, and Face Recognition with Applications*, 25 Sensors 1410 (2025), available at https://pubmed.ncbi.nlm.nih.gov/40096196/ (last visited Jan. 18, 2026);
[100] N.Y.C. ADMIN. CODE § 14-188(a).
[101] *See* N.Y.C. ADMIN. CODE § 14-188(c).
[102] The facts in this section are summarized from Appendix B at 11.

Internal Affairs Bureau given authority to investigate allegations of misuse. Finally, Integrity Control Officers in each command are responsible for the overall security and integrity of recorded media and computer systems.

The Facial Recognition IUP also includes the following regarding audits: "Requests for focused audits of computer activity from IAB, Commanding Officers, [Integrity Control Officers], Investigations Units, and others, may be made to the Information Technology Bureau."

*The NYPD's Practices and Procedures*:

The NYPD confirmed that no individual so authorized has requested a "focused audit of computer activity" related to facial recognition technology. Separately, given the effective date of the 2025 amendments to the POST Act, the mandated audit of the use of Facial Recognition Policy falls outside the temporal scope of this review.

Following the 2025 amendments to the POST Act, the NYPD is *required* to include audits as an oversight mechanism for its facial recognition use. As such, OIG-NYPD recommends as follows:

> **Recommendation #16:** The NYPD should adopt a policy requiring annual audits of its facial recognition analyses in accordance with the 2025 amendments to the POST Act and amend the Facial Recognition Impact and Use Policy consistent with the new policy.

This policy is not only required to come into compliance with the POST Act, but it will also help the NYPD assess whether its facial recognition investigators need additional training and whether the NYPD's facial recognition analyses result in any disparate impacts, such as misidentification of certain categories of individuals. When adopting this policy, the NYPD should also consider reprising audits for accuracy of its facial recognition analyses.[103]

## I. Health and Safety Effects

The ninth requirement in the POST Act is that Impact and Use Policies must address both: "(a) any tests or reports regarding the health and safety effects of the surveillance technology" and "(b) any known physical safety hazards of the surveillance technology . . . or a statement that no such hazards have been identified after a search for relevant information."[104]

*The Facial Recognition IUP*[105]: The Facial Recognition IUP states in full: "There are no known tests or reports regarding the health and safety effects of facial

[103] It appears that the NYPD has conducted such audits on at least one occasion in the past. *See* Clare Garvie, *Garbage In, Garbage Out Flawed Face Data* (2019), https://www.flawedfacedata.com/ (last visited Oct 31, 2025) (discussing documents received in response to a 2016 FOIL request to the NYPD that include a discussion of historical facial recognition identifications and misidentifications).
[104] N.Y.C. ADMIN. CODE § 14-188(a).
[105] Information in this section is taken from Appendix B at 11.

recognition technology. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of facial recognition technology."

*The NYPD's Practices and Procedures*: To assess the accuracy of the Facial Recognition IUP's health and safety reporting, OIG-NYPD conducted a literature review related to research on the health and safety of facial recognition technology.

The Office found no tests or reports indicating that facial recognition technologies in and of themselves pose any health, safety, or physical hazards to the public.

### J. Potential Disparate Impacts

The last requirement for Impact and Use Policies laid out in the POST Act is that they address "any potentially disparate impacts of the surveillance technology and surveillance technology impact and use policy on any protected groups as defined in the New York city human rights law."[106]

*The Facial Recognition IUP*[107]: The Facial Recognition IUP begins by recognizing that some studies have found that there are variations in accuracy for some facial recognition technologies as between groups of different races and genders. However, the Policy notes that its use of technology has not shown any potential for disparate impacts, given the "significant safeguards" the NYPD has adopted, including: (1) the integration of multiple human reviewers into the analysis process; (2) the limitations on the manner in which facial recognition can be used; and (3) the use of facial recognition technologies "which have been evaluated by the National Institute of Standards and Technology ("NIST") for matching efficiency and accuracy." The NYPD also notes that it is committed to impartial law enforcement in compliance with City law and the State and Federal Constitutions.

*The NYPD's Practices and Policies*: NIST evaluates facial recognition algorithms by analyzing algorithm accuracy, false match rates, demographic performance differences, and how systems perform under real-world conditions.[108] Through its Face Recognition Technology Evaluation, NIST provides independent performance benchmarks that inform government agencies and policymakers about the reliability and limitations of facial recognition technology.[109] Importantly, a NIST evaluation is a performance measurement, not a product endorsement.[110] Because

[106] N.Y.C. ADMIN. CODE § 14-188(a).
[107] Information in this section is taken from Appendix B at 12.
[108] *See* NAT. INST. STANDARDS & TECH. SPECIAL PUBL'N., *available* at https://www.commerce.gov/bureaus-and-offices/nist (last visited Feb. 26, 2026).
[109] *See* NAT. INST. STANDARDS & TECH. SPECIAL PUBL'N., *Face Recognition Technology Evaluation (FRTE) 1:N Identification, available at* https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (last visited Feb. 26, 2026).
[110] *See* NAT. INST. STANDARDS & TECH. SPECIAL PUBL'N., *available at https://pages.nist.gov/frvt/agreements/frvt_participation_agreement.pdf*, 2, (last visited August 21,

developers worldwide submit algorithms continuously and frequently retrain them, performance results – including demographic differentials – are subject to change.[111] Therefore, a NIST result is a measurement of a particular algorithm version at a given time. As a result, an algorithm that ranked well upon initial acquisition may perform differently in subsequent evaluations.

During its evaluation, the Office requested information from the NYPD to show how often the NYPD reviewed NIST's evaluation of their acquired facial recognition technology products. The NYPD reported that it had no program to conduct any such review. OIG-NYPD notes that, through NIST, the NYPD has the opportunity to periodically assess its vendor's algorithms to ensure that accuracy and efficiency remain consistent with initial acquisition levels. Accordingly, OIG-NYPD recommends as follows:

> **Recommendation #17:** The NYPD should regularly review its facial recognition technology vendor's National Institute of Standards and Technology evaluations to verify ongoing performance consistency.

These periodic checks would ensure that the Facial Recognition IUP's assertion that the NYPD's facial recognition algorithms "have been evaluated by NIST for matching efficiency and accuracy" remains accurate.

## V. Conclusion

Facial recognition technology has become an increasingly important tool in modern law enforcement, but not a tool that is without critics. Although the law places very few constraints on how and when the NYPD may use facial recognition technology, the NYPD has adopted policies that limit the NYPD's use of this technology significantly, as embodied in the Facial Recognition IUP. As discussed above, during this POST Act audit, OIG-NYPD determined that, with certain important exceptions, the NYPD is broadly compliant with its Facial Recognition IUP. This report offers the NYPD seventeen recommendations concerning its Facial Recognition IUP that will improve the NYPD's compliance, particularly with recent amendments to the POST Act passed in 2025. These recommendations are as follows:

> **Recommendation #1:** The NYPD should amend the Facial Recognition Impact and Use Policy to include the names of the three facial recognition products in use at the NYPD.
>
> **Recommendation #2:** The NYPD should amend the Facial Recognition Impact and Use Policy to enumerate the photo repositories associated with each of the facial recognition products it uses, as well as to identify

2026) ("Results shown from NIST do not constitute an endorsement of any particular system, product, service, or company by NIST.").

[111] *See* NAT. INST. STANDARDS & TECH. SPECIAL PUBL'N., *Face Recognition Technology Evaluation (FRTE) 1:N Identification, available at* https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (last visited Feb. 26, 2026).

specifically from where the photographs contained in the photo repositories are obtained.

**Recommendation #3:** The NYPD should amend its Facial Recognition Impact and Use Policy to specifically identify which Bureaus have access to facial recognition technology, what those Bureaus do, and who they serve.

**Recommendation #4:** The NYPD should update Patrol Guide 212-129 to instruct personnel to request facial recognition analysis only from the authorized unit within their assigned Bureau.

**Recommendation #5:** The NYPD should ensure that facial recognition analysis logs in both the Enterprise Case Management System and the Intelligence Division Case Management System are standardized to capture consistent and accurate data collection across all entries.

**Recommendation #6:** The NYPD should update Patrol Guide 212-129 to memorialize the Facial Recognition Impact and Use Policy's guidelines regarding acceptable image enhancement techniques.

**Recommendation #7:** The NYPD should establish and document an authorization process requiring facial recognition investigators to obtain permission from the Chief of Detectives or Chief of Intelligence (depending on the relevant Bureau the facial recognition investigator is assigned to) prior to editing probe images beyond standard parameters.

**Recommendation #8:** The NYPD should implement a mandatory documentation process to log all probe image modifications in compliance with the 2025 POST Act amendments.

**Recommendation #9:** The NYPD should amend the Facial Recognition Impact and Use Policy and Patrol Guide 212-129 to include guidance on how to select which facial recognition software program to use when conducting facial recognition analyses.

**Recommendation #10**: The NYPD should amend the Facial Recognition Impact and Use Policy, Patrol Guide 212-129, and other related policies to (1) clearly indicate which individual(s) in the Intelligence and Counterterrorism Bureau are authorized to review facial recognition analysis requests to outside agencies; and (2) require formal documentation of the outside request process in both the Detective Bureau and the Intelligence and Counterterrorism Bureau, including whether each request was approved or denied along with the reasoning behind the decision.

**Recommendation #11:** The NYPD should amend the Facial Recognition Impact and Use Policy and all associated policies to require

mandatory supervisory review and blind peer review for all facial recognition analyses, and to mandate the documentation of reviewer names and result outcomes.

**Recommendation #12:** The NYPD should update the Facial Recognition Impact and Use Policy and related policies to codify procedures for facial recognition requests performed by outside entities, establish guidelines for officers' use of the results, and ensure that this process is documented and auditable.

**Recommendation #13:** The NYPD should adopt procedures in Patrol Guide 212-129 sufficient to ensure that FIS and the Intelligence Division do not process the same outside facial recognition requests.

**Recommendation #14:** The NYPD should provide training on the operation of facial recognition technology and related NYPD policies regarding the use of such technology to all investigators authorized to conduct searches.

**Recommendation #15:** The NYPD should establish recertification requirements involving additional training at periodic intervals for its facial recognition investigators.

**Recommendation #16:** The NYPD should adopt a policy requiring annual audits of its facial recognition analyses in accordance with the 2025 amendments to the POST Act and amend the Facial Recognition Impact and Use Policy consistent with the new policy.

**Recommendation #17:** The NYPD should regularly review its facial recognition technology vendor's National Institute of Standards and Technology evaluations to verify ongoing performance consistency.

OIG-NYPD thanks the NYPD for its cooperation with this audit.

## Appendix A: Legal Aid Society Letter

THE LEGAL AID SOCIETY CRIMINAL DEFENSE

Digital Forensics Unit
49 Thomas Street
New York, NY 10013
(212) 732-5000
https://www.legalaidnyc.org/

Cell (929) 536-1637
LMoraff@legal-aid.org

Alan Levine
*President*

Twyla Carter
*Attorney-in-Chief*
*Chief Executive Officer*

Justine M. Luongo
*Chief Attorney*
Criminal Practice

David Loftis
*Attorney-in-Charge*
Post-Conviction & Forensic Litigation

August 25, 2025

Via Email & U.S. Mail
Inspector General Jeanene Barrett
Office of the Inspector General for the
New York City Police Department
New York City Department of Investigation
180 Maiden Lane
New York, NY 10038

Re: Violations of NYPD's Facial Recognition Policies

Dear Inspector General Jeanene Barrett,

We write to respectfully request that you open an investigation into the New York City Police Department's (NYPD's) violations of its facial recognition technology policies and include the details and results of your investigation in the next annual audit pursuant to the Public Oversight of Surveillance Technology Act (Local Law 65 of 2020).

Facial recognition technology is utilized when an investigating officer has a photo of a criminal suspect but does not know their identity. The officer sends that image (the "probe image") to the NYPD's Facial Identification Section (FIS), and FIS uses its facial recognition technology to compare the probe image to the photos in the NYPD's photo repository. The photo repository allegedly contains only arrest and parole photos of individuals who have been charged with a New York crime.

According to the NYPD's own Impact and Use Policy for facial recognition, "[t]he use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Department, Chief of Detectives, or Deputy Commissioner, Intelligence and Counterterrorism." Facial Recognition: Impact and Use Policy, at 6 (Nov. 24, 2023)[1] (hereinafter "IUP"); accord Patrol Guide, Procedure No. 212-129 at 363.[2] If there is such approval for a previously unprescribed use of facial recognition technology, the NYPD must write an addendum to the existing IUP that describes the additional uses of facial recognition technology. IUP at 7.

Despite these clear limitations on comparing probe images to any images outside the NYPD's own photo repository, The Legal Aid Society has become aware that, in some cases where the NYPD's

[1] Available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_11.24.23.pdf.
[2] Available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide2.pdf.

Facial Identification Section (FIS) finds no match in the NYPD's photo repository, the Special Activities Unit (SAU) in the Intelligence Division uses facial recognition technology and finds a possible match. For example, earlier this year, when the NYPD was investigating a case of public lewdness, a detective sent a surveillance video to FIS in order to identify a suspect in the video. FIS determined that there was no match found for the unidentified suspect. The investigating detective's DD5 states that she was advised of an FIS no match notification. But just a few hours later, there was another DD5 from the same detective stating that she was uploading a possible FIS match. A review of ECMS records clearly shows that possible match came from SAU—not FIS.

This match led to the wrongful arrest of Trevis Williams, a Black man who did not match the physical description given by the victim, but was nevertheless arrested for the crime based on the facial recognition match and an unnecessarily and unduly suggestive identification procedure. Mr. Williams was falsely arrested, and his life and job prospects were put on hold—all because of the NYPD's adoption of a biased surveillance tool and disregard for the policies governing its use.

We do not know how or why SAU is able to find possible matches when FIS is not. We do not know whether SAU is relying only on the NYPD's photo repository—and making changes in order to get a possible match—or using other sets of photos, although we have reason to believe that at least on some occasions they are using the NY/NJ High Intensity Drug Trafficking Area's database of photos. We do not know whether SAU or FIS is getting the required approval to use facial recognition technology to compare probe images to photos outside of the NYPD's photo repository. We do not know whether or how SAU's facial recognition technology differs from FIS's—in part because SAU has not disclosed this information, even when it is responsible for identifying matches in criminal cases.

We were also alarmed to learn that NYPD circumvents its facial recognition policies by relying on other entities altogether to use facial recognition technology and then share the results with the NYPD. *See* Samantha Maldonado, *NYPD Bypassed Facial Recognition Ban to ID Pro-Palestinian Student Protester*, The City (Jul. 18, 2025).[3] For example, on June 3, 2024, an FDNY fire marshal sent an NYPD detective an email saying he ran a photo from Crime stoppers "through our facial and it came back to this guy who graduated from Ossining High School in 2022," and included screenshots of facial recognition matches. *People v. Ahmed*, No. CR-017044-24NY (Crim. Ct. Jun. 17, 2025).[4] In the same email chain, the fire marshal told the detective that if he could get a name, then the fire marshal could "get the DL photo for [him]." *Id.* The detective replied with a name, date of birth, and driver's license number; the fire marshal replied "Bingo," indicating he had found a match. *Id.* Judge Morales recognized this as a case of the FDNY doing "what the NYPD could not," as "the NYPD does not permit a facial recognition search to extend as widely as it did in this case."

[3] Available at https://www.thecity.nyc/2025/07/18/nypd-fdny-clearview-ai-ban-columbia-palestinian-protest/.
[4] Available at https://www.nycourts.gov/reporter/3dseries/2025/2025_51047.htm#:~:text=The%20defendant%20was%20identified%20in%20early%20June%202024,to%20dismiss%20the%20felony%20on%20September%2023%2C%202024.

*Id.* The court further emphasized that "[w]here the state routinely gathers, searches, seizes, and preserves colossal amounts of information, transparency must remain a touchstone, lest fairness be lost." *Id.*

NYPD's circumvention of its facial recognition policies is particularly unnerving given the rising number of cases in which clients, like Mr. Williams, were falsely arrested based on faulty facial recognition matches. We are aware of multiple such cases, and we are gravely concerned that the cases we have identified are only the tip of the iceberg. The NYPD's vague IUP does not adequately address serious concerns about the accuracy and fairness of facial recognition technology. High profile cases of individuals being wrongfully arrested based on facial recognition technology have shed light on just how devastating the consequences of this technology can be—particularly for Black individuals. *See, e.g.*, Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023);[5] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022).[6] As your office has noted, there is significant public concern surrounding the use of facial recognition technology leading to increased bias in policing. A 2022 study by Amnesty International found that the use of facial recognition technology reinforced discriminatory stop and frisk policing in New York. Amnesty International Press Release, *New Research Finds Facial Recognition Technology Is Reinforcing Racist Stop-and-Frisk Policing in New York* (Feb. 14, 2022).[7] Your office has recognized the need for clear policies with respect to the NYPD's use of facial recognition technology as well as audits, DOI's Ninth Annual Report at 15–16,[8] and the City Council's passage of Intro 233 confirms the urgency of those measures.

We respectfully request that your office conduct an expeditious and thorough investigation into the NYPD's facial recognition policies and any methods employed to circumvent its own policies, including through reliance on units outside of FIS and other city agencies or departments.

Please do not hesitate to contact our office if you would like to discuss these concerns or have any questions for us.

[5] Available at https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.
[6] Available at https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
[7] Available at https://www.amnestyusa.org/press-releases/facial-recognition-technology-reinforcing-racist-policing-new-york/
[8] Available at https://www.nyc.gov/assets/doi/reports/pdf/2023/13OIGNYPDRpt.Release.03.30.2023.pdf.

Sincerely,

Jennvine Wong, Esq.
49 Thomas Street
New York, NY 10013
(212) 577-3309
JWong@legal-aid.org

Laura Moraff, Esq.
49 Thomas Street
New York, NY 10013
(929) 536-1637
LMoraff@legal-aid.org

Cc: NYC Council Speaker Adrienne E. Adams (via email & U.S. mail)
NYC Council Committee on Public Safety Chair Yusef Salaam (via email & U.S. mail)
NYC Council Committee on Technology Chair Jennifer Gutiérrez (via email & U.S. mail)
NYC Council Committee on Oversight and Investigations Chair Gale A. Brewer (via email & U.S. mail)

**Justice in Every Borough.**

## Appendix B: NYPD's Facial Recognition IUP – February 2026

# FACIAL RECOGNITION: IMPACT AND USE POLICY

**UPDATED: FEBRUARY 4, 2026**

**FACIAL RECOGNITION:**
**IMPACT & USE POLICY**

NYPD

**SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY**

| Update | Description of Update |
|---|---|
| Removed statement that facial recognition software does not use artificial intelligence and machine learning. | Public comments highlighted a lack of industry-standard definitions for artificial intelligence and Machine Learning. |
| Expanded upon facial recognition capabilities section. | Added language clarifying facial recognition capabilities. Added language how facial recognition is not integrated with other NYPD technologies. Added language describing the photo repository. |
| Expanded upon facial recognition rules of use. | Added language clarifying facial recognition rules of use. Added language describing facial identification; the human review of potential possible match candidates. |
| Expanded upon facial recognition safeguard and security measures. | Added language regarding information security. Added language to reflect the removal of access to facial recognition technologies when job duties no longer require access. |
| Expanded upon facial recognition data retention. | Added language to reflect NYPD obligations under federal, state, and local record retention laws. |
| Expanded upon external entities section. | Added language to reflect the NYPD's obligations under the local privacy laws. |
| Minor grammar changes. | Minor syntax edits were made. |

**FACIAL RECOGNITION:**
**IMPACT & USE POLICY**

NYPD

**FACIAL RECOGNITION ADDENDUM**

| Date of Addendum | Addendum Description |
|---|---|
| October 26, 2023 | Updated to reflect current policies and functions of Facial Recognition technology used by the NYPD.<br><br>Minor syntax edits were made. |
| November 24, 2023 | Disparate impacts of the impact and use policy section updated to reflect findings of major improvements in the accuracy of the technology. |

**FACIAL RECOGNITION REVISION**

| Date of Revision | Description of Revision |
|---|---|
| February 4, 2026 | This impact and use policy was revised to comply with the recently passed amendment to the POST Act, Local Law 56 of 2025. |

**FACIAL RECOGNITION:**
**IMPACT & USE POLICY**

NYPD

## ABSTRACT

Facial recognition is a digital technology that the New York City Police Department (NYPD) uses to compare probe images to an arrest and parole photo gallery for specific, legitimate law enforcement purposes. Used in combination with human analysis and additional investigation, facial recognition technology is a valuable tool in solving crimes and increasing public safety.

Facial recognition technology used by the NYPD is routinely evaluated by the National Institute of Standards and Technology (NIST) for efficiency and accuracy, as is routine in the industry. NYPD facial recognition investigators are trained, and access to the technology itself is limited solely to those personnel. No one has ever been arrested solely based on facial recognition results by the NYPD.

The NYPD produced this impact and use policy because facial recognition technology processes biometric information.

## CAPABILITIES OF THE TECHNOLOGY

Since 2011, the NYPD has successfully used facial recognition technology to investigate criminal activity and increase public safety. The NYPD uses facial recognition to aid in the identification of suspects whose images have been recorded on-camera at robberies, burglaries, assaults, shootings, and other crimes. The NYPD also uses facial recognition to aid in the identification of persons unable to identify themselves (e.g., persons experiencing memory loss or unidentified deceased persons). NYPD uses facial recognition technology manufactured by Dataworks+ (also known as Clearview Data Systems) and Idemia.

NYPD investigators often obtain video and photos over the course of an investigation. If a video or photo contains an image of the face of an unknown individual, the image can be submitted for facial recognition analysis in accordance with NYPD facial recognition policy.

Known as a "probe image," NYPD facial recognition software compares the probe image to a controlled and limited group of photos already within lawful possession of the NYPD, called the "photo repository." The photo repository only contains arrest and parole photographs of individuals that have been charged with a crime where a criminal court has jurisdiction. The photo repository does not contain photos related to arrests that have been sealed. Probe images are never entered into and do not become part of the photo repository.

NYPD facial recognition technology analyzes inputted probe images. The software generates a pool of possible match candidates that are manually reviewed by specially trained NYPD facial recognition investigators to determine the differences and similarities between a probe image and a potential match.

The NYPD does not perform real-time facial recognition. NYPD video cameras or systems (e.g., CCTV cameras, unmanned aircraft systems, and body worn cameras, etc.) cannot conduct real-time facial recognition. Facial recognition technology does not use any additional biometric measuring technologies.

## RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD facial recognition technology must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

The facial recognition process may generate investigative leads through a combination of automated biometric comparisons and human analysis. It does not by itself establish a basis for a stop, probable cause to arrest, or to obtain a search warrant.

***Operational Use:*** Facial recognition technology must only be used for legitimate law enforcement purposes. Authorized uses of facial recognition technology are limited to the following:

1. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime;
2. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;
3. To identify a deceased person;
4. To identify a person who is incapacitated or otherwise unable to identify themselves;
5. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, who appears to be using someone else's identification, or a false identification; or
6. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

For criminal investigations, a possible facial recognition match serves as a lead for additional steps. An arrest will not be made until the assigned investigator establishes, with other corroborating evidence, probable cause to believe that the suspect identified as a possible match is the perpetrator in an alleged crime.

***Request for Use:*** When an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, the investigator must submit a request for facial recognition analysis. Specifically, the request is made for the image depicting the face of the unknown person (the probe image) to be compared to photos in the photo repository. The request for facial recognition analysis must include a case or complaint number for the matter under investigation and the probe image(s) of the unidentified person.

The facial recognition investigator must confirm that the basis of the request is in compliance with the enumerated list of authorized uses of facial recognition technology. That confirmation must be documented by the requesting investigator in the appropriate NYPD case management system.[1] The facial recognition investigator will select a probe image of the unidentified person from the submitted images. If image quality is not suitable for facial recognition comparison, the requesting investigator will be notified and given the opportunity to submit additional images.

[1] For additional information on case management systems, please refer to the case management systems impact and use policy.

The facial recognition investigator will run a search using the facial recognition software for comparison of the probe image to the photo repository. The software generates a pool of possible match candidates.

A "possible match candidate" is a potential suspect who is identified through a complete facial recognition analysis, which includes facial recognition technology, visual comparison, peer review, background investigation and supervisory review. A possible match candidate shall be treated as an investigative lead only. It does not by itself establish probable cause to make an arrest, or obtain an arrest or search warrant. Corroborating information must be developed through additional investigation by the assigned investigator.

More specifically, 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 probe 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. A detailed background check is conducted by the requesting investigator to corroborate a possible match.

Next, a possible match candidate is submitted for peer review to 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.

If there is a difference of opinion with the findings, the 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.

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 case file in the case management system. The possible match report includes the probe image, 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.

Probe images are only minimally adjusted through brightness correction, cropping, or rotating for clarity purposes. Probe images are never materially altered or enhanced in a manner that affects biometric identifiers.

Images obtained from body-worn cameras[2] worn by NYPD officers are not routinely submitted for facial recognition analysis. For example, the NYPD does not use 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

[2] For more information about NYPD body-worn cameras ("BWC"), please see the BWC impact and use policy.

suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

***Court Authorization:*** The NYPD does not seek court authorization prior to the use of facial recognition technology since the tool conducts analysis of images that have been lawfully obtained by the NYPD.

***Additional Guidelines:*** The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case, for an articulable reason, by the Chief of Department, Chief of Detectives, and Deputy Commissioner of Intelligence and Counterterrorism.

In situations where use of a NYPD facial recognition technology has not been foreseen or prescribed in policy, the Chief of Department, Chief of Detectives, and Deputy Commissioner of Intelligence and Counterterrorism will decide if use is appropriate and lawful.

The NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies. NYPD investigations involving political activity are conducted by the Intelligence Division, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Revised *Handschu* Guidelines.

As with all NYPD operations, no person will be the subject of police action because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

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

***Addendum Obligation:*** In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of facial recognition technology.

## SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

***Data Safeguard & Security Measures:*** Access to facial recognition technology is limited to NYPD facial recognition investigators. Access to facial recognition technology is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

Facial recognition investigators using the software are first authenticated by username and password. Facial recognition investigators are provided with access only after completing mandatory training related to use of the technology.

Information resulting from use of facial recognition technology is retained within NYPD computer and case management systems. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful

duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case-by-case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties from unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

## POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS, & USE OF THE DATA

The results of facial recognition analysis may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigation, and disciplinary proceedings. Facial recognition analysis results relevant to a case or investigation are stored in appropriate NYPD computer or case management systems. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management is limited to personnel who have an articulable need to access the system in furtherance of lawful duty.

The NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains

and disposes of records pursuant to this schedule. The retention period of a "case investigation record" depends on its classification and is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought.

The misuse of data will subject employees to administrative and potentially criminal penalties.

## POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request information obtained from the NYPD's use of facial recognition technology pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of the law and NYPD policy.

## EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by NYPD's facial recognition technology.

An external law enforcement agency may request that the NYPD run a facial recognition search in connection with an active criminal investigation. Any such request is documented, and the NYPD will run such a search in accordance with Department policy and procedure. The Department does not have an agreement with any external entities to run facial recognition searches on their behalf, and no external entities have the ability to run facial recognition searches through the Department's systems.

If the use of facial recognition technology produces information related to a criminal case, the NYPD will turn it over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the information to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information contained in NYPD computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide information to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Such information will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from facial recognition technology may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community concern.

Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such

individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;
5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;
6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime;
7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

***Vendors & Contractors:*** The NYPD purchases facial recognition technology and associated equipment or software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD facial recognition technology associated program or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If facial recognition data is disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer within 24 hours. The NYPD must make reasonable efforts to notify individuals affected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publicly available online.

## TRAINING

NYPD personnel utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, and the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training.

## INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of facial recognition technology, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing facial recognition technology are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

## HEALTH & SAFETY REPORTING

There are no known tests or reports regarding the health and safety effects of facial recognition technology. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of facial recognition technology.

## DISPARATE IMPACTS OF THE TECNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that facial recognition technology is used effectively and responsibly. The NYPD does not believe that the technology has shown any potentially disparate impacts on any protected groups as defined in the New York City Human Rights Law.

Some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asians Americans, women, and groups other than non-white males. However, over the last half decade, NIST has identified major improvements in the accuracy of facial recognition software. Moreover, NYPD policy requires that facial recognition software recommendations be analyzed by multiple human reviewers before a possible match candidate can be conveyed to an investigator. Even when an investigator is informed that a possible match

candidate has been identified, it only serves as a lead for additional investigative steps. Identification of a possible match candidate does not establish cause to arrest or obtain a search warrant.

The safeguards and audit protocols built into this impact and use policy for facial recognition technology mitigate the risk of partial and biased law enforcement. NYPD 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 probe image, 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.

The NYPD only uses facial recognition algorithms which have been evaluated by NIST for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for facial recognition are periodically updated as necessary based on subsequent NIST evaluations. Based on these safeguards, any theoretical risks of facial recognition are effectively mitigated and do not result in disparate impacts.

The NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws.

Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action. Should an officer initiate enforcement action against a person, motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not only race, age, and gender, but other identifying characteristics or information.

# Appendix C: Patrol Guide 212-129, Facial Recognition Technology

**PATROL GUIDE**

| Section: Command Operations | | Procedure No: 212-129 |
|---|---|---|
| **FACIAL RECOGNITION TECHNOLOGY** | | |
| DATE EFFECTIVE: 12/02/22 | LAST REVISION: I.O. 116 | PAGE: 1 of 4 |

**PURPOSE** To ensure the use of facial recognition technology balances the need for effective, accurate law enforcement investigations, and the need to respect the privacy of citizens.

**SCOPE** Facial recognition technology enhances the ability to investigate criminal activity and increases public safety. The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

**DEFINITIONS** AUTHORIZED USES - Facial recognition technology must only be used for legitimate law enforcement purposes. Specifically, the following are the only authorized uses for employing facial recognition technology:

a. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime,
b. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity,
c. To identify a deceased person,
d. To identify a person who is incapacitated or otherwise unable to identify themselves,
e. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification, or
f. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot, etc.).

PROBE IMAGE - An image of an unidentified person obtained by the assigned investigator from witnesses, victims, or other reliable sources.

PHOTO REPOSITORY - The controlled and limited group of images against which the probe image is compared. The photo repository only contains arrest and parole photographs. It is stored in a designated, and approved, law enforcement database, and access is restricted to authorized users.

BACKGROUND CHECK - A Real Time Crime Center, Facial Identification Section (RTCC-FIS) investigator evaluates the reliability of a potential match between the probe image and an image from the photo repository. This includes an assessment of available information about the potential match, and relevant details of the investigation.

NEW • YORK • CITY • POLICE • DEPARTMENT

**PATROL GUIDE**

| PROCEDURE NUMBER: | DATE EFFECTIVE: | LAST REVISION: | PAGE: |
|---|---|---|---|
| 212-129 | 12/02/22 | I.O. 116 | 2 of 4 |

**DEFINITIONS (continued)**

VISUAL COMPARISON - A RTCC-FIS investigator visually compares the differences and similarities between a probe image and a potential match from the photo repository for the purpose of evaluating whether they represent the same person. In general, during this process, an investigator/supervisor compares facial characteristics (e.g., eyes, ears, nose, chin, mouth, hair, overall facial structure, any scars, marks, blemishes, or tattoos, etc.) and general characteristics, such as overall complexion, gender, and age.

POSSIBLE MATCH CANDIDATE - A potential suspect who is identified through a complete facial recognition analysis, which includes facial recognition technology, visual comparison, background investigation and supervisory review. A possible match candidate shall be treated as an investigative lead only. It does not by itself establish probable cause to make an arrest, or obtain an arrest or search warrant. Corroborating information must be developed through additional investigation by the assigned investigator.

**PROCEDURE**

When an investigator obtains an image depicting the face of an unidentified suspect, victim or witness, and intends to identify the individual using facial recognition technology, which includes any digital comparison of the probe image to photos stored in the photo repository, the assigned investigator must submit a request to the RTCC-FIS for facial recognition analysis:

FACIAL IDENTIFICATION SECTION PERFORMS FACIAL RECOGNITION ANALYSIS:

**ASSIGNED INVESTIGATOR**

1. Obtain image(s)/video(s) of individual to be identified.
   a. If video is submitted, include associated software/player.
   b. If image is from internet/social media, include site link.
2. Upload image(s) to Enterprise Case Management System (ECMS) and submit request to Real Time Crime Center-Facial Identification Section (RTCC-FIS) for facial recognition analysis via an **FIS Request DD5**.

***NOTE*** *Investigators who do not have access to the Enterprise Case Management System (ECMS) may contact RTCC-FIS via phone or email. Investigators must provide a case or **COMPLAINT REPORT (PD313-152)** number. RTCC-FIS will generate an **FIS Request DD5**.*

**RTCC-FIS SUPERVISOR**

3. Assign FIS number to request upon receipt of **FIS Request DD5** via ECMS, and direct RTCC-FIS investigator to review request.

**RTCC-FIS INVESTIGATOR**

4. Confirm underlying basis for request is in compliance with authorized uses of facial recognition technology.
   a. Document confirmation in ECMS.
5. Select probe image of individual to be identified from images submitted.
   a. If image quality is unsuitable for facial recognition comparison, notify the assigned investigator via **FIS Image Rejection Report**.
   b. Permit assigned investigator to submit additional images.

**NEW • YORK • CITY • POLICE • DEPARTMENT**

**PATROL GUIDE**

| PROCEDURE NUMBER: | DATE EFFECTIVE: | LAST REVISION: | PAGE: |
|---|---|---|---|
| 212-129 | 12/02/22 | I.O. 116 | 3 of 4 |

**RTCC-FIS INVESTIGATOR (continued)**

6. Run query using facial recognition technology for comparison of probe image to images stored in photo repository, and generate pool of possible match candidates.
7. Review and analyze results by performing a visual comparison.
8. Perform detailed background check to confirm reliability of match, if possible match candidate is identified.
9. Submit possible match candidate for peer review.

**RTCC-FIS SUPERVISOR**

10. Conduct final review of possible match candidate, and approve, if appropriate.
11. Direct RTCC-FIS investigator to provide possible match candidate to assigned investigator via **FIS Possible Match Report**, if in agreement with findings.
12. Direct RTCC-FIS investigator to continue investigation for possible match candidate, if not in agreement with findings of RTCC-FIS investigator.
    a. Direct RTCC-FIS investigator to report negative results to assigned investigator via **FIS No Match Report**, if possible match candidate is not identified or approved by supervisor.

**RTCC-FIS INVESTIGATOR**

13. Prepare **FIS Possible Match Report** and upload to assigned investigator's ECMS case file, if supervisor confirms possible match candidate.
    a. **FIS Possible Match Report** shall include probe image, and notification stating that 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.
    b. Forward **FIS Possible Match Report** using same method used to submit request for facial recognition analysis, if request is from outside law enforcement agency.
14. Retain all records of facial recognition searches, including associated FIS case number, reason each search was requested, details, and search results, and upload them into the ECMS case file.

**ASSIGNED INVESTIGATOR**

15. Conduct further investigation to determine whether possible match candidate is connected to, or involved in, incident under investigation, upon receipt of **FIS Possible Match Report** in order to establish probable cause.
16. Continue investigation, (i.e., obtaining additional suitable images for another submission to RTCC-FIS), if no possible match candidate was determined, or image was rejected.

***ADDITIONAL DATA***

*The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited, unless approval is granted for such analysis in a specific case for an articulable reason, by the Chief of Detectives, Intelligence and Counterterrorism Bureau, or Chief of Intelligence. Approval, including reasoning, must be digitally documented in the appropriate Department case file system (e.g., ECMS, etc.). Members of the service will comply will all relevant Department directives regarding criminal discovery, as appropriate.*

**NEW • YORK • CITY • POLICE • DEPARTMENT**

**PATROL GUIDE**

| PROCEDURE NUMBER: | DATE EFFECTIVE: | LAST REVISION: | PAGE: |
|---|---|---|---|
| 212-129 | 12/02/22 | I.O. 116 | 4 of 4 |

***ADDITIONAL DATA (continued)***

*RTCC-FIS and Detective Squad supervisors shall comply with P.G. 219-14, "Department Computer Systems" to evaluate and monitor compliance with this procedure by investigators who utilize facial recognition technology.*

*All records related to facial recognition requests and results will be subject to privacy, confidentiality, and dissemination restrictions, as per P.G. 212-76, "Information Concerning Official Business of Department," as well as all related procedures and applicable local and federal laws/rules. Members of the service may not disclose identifying information without prior authorization. Any questions concerning the disclosure of photos or information regarding facial recognition should be directed to the Legal Bureau, Director of Privacy Matters.*

*Members of the Detective Bureau should direct all requests from outside agencies to RTCC-FIS on an "FIS Outside Agency Form." A copy of a complaint report from another law enforcement agency must be submitted with the "FIS Outside Agency Form."*

*Members of the Intelligence Division who have authorized access to facial recognition software must strictly comply with this procedure when utilizing the technology, and will abide by Handschu Guidelines whenever they apply.*

***RELATED PROCEDURES***

*Information Concerning Official Business of Department (P.G. 212-76)*
*Department Computer Systems (P.G. 219-14)*

***FORMS AND REPORTS***

***COMPLAINT REPORT (PD313-152)***
***FIS Request DD5***
***FIS Possible Match Report***
***FIS No Match Report***
***FIS Image Rejection Report***

NYPD

NEW • YORK • CITY • POLICE • DEPARTMENT