DIGITAL FINGERPRINT SCANNING DEVICES: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that digital fingerprint scanning devices do not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon digital fingerprint scanning devices rules of use.	Added language clarifying digital fingerprint scanning devices rules of use.
Expanded upon digital fingerprint scanning devices safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to digital fingerprint scanning devices when job duties no longer require access.
Expanded upon digital fingerprint scanning devices data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon digital fingerprint scanning devices external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

DIGITAL FINGERPRINT SCANNING DEVICES ADDENDUM

Date of Addendum	Description of Addendum
April 11, 2023	NYPD smartphones issued to certain personnel assigned to the Criminal Justice, Detective, Patrol, Transit, and Housing Bureaus have access to a digital fingerprint scanning application on their device.

DIGITAL FINGERPRINT SCANNING DEVICES 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.

ABSTRACT

The New York City Police Department (NYPD) uses digital fingerprint scanning devices to confirm identification, perform warrant and criminal history background checks, and provide police with potential leads in criminal investigations.

Fingerprints are a common biometric measurement, inextricably connected to the modern world of policing and law enforcement. The NYPD uses stationary and mobile identification devices, in addition to a smartphone application, to digitally scan fingerprints.

The NYPD produced this impact and use policy because NYPD digital fingerprint scanning devices have the ability to process biometric information.

CAPABILITIES OF THE TECHNOLOGY

NYPD digital fingerprint scanning devices are inkless electronic devices capable of recording fingerprints in a digitized format. Compared to traditional ink fingerprinting methods, use of digital fingerprint scanning devices improves the quality of fingerprint scans and reduces the amount of time required for the NYPD to both scan fingerprints and receive any associated information. Additionally, digital fingerprint scanning devices allow personnel to efficiently retake a print several times, if necessary, to ensure a quality image is recorded.

An "Automated Fingerprint Identification System" (AFIS) is a local, state, or national database containing two types of fingerprint records: known fingerprints and evidence fingerprints. Known fingerprints are fingerprints that have been previously connected to an individual. Evidence fingerprints are collected from one or more crime scenes, or other relevant locations, but do not yet have a known identity attached to them.

When a fingerprint is submitted for comparison, the internal system processor automatically compares the fingerprints captured through digital fingerprint scanning devices with fingerprints contained in the NYPD's local AFIS for identification purposes. The fingerprint is subsequently compared with the state AFIS maintained by the NYS Division of Criminal Justice Services (DCJS) and the national AFIS maintained by the Federal Bureau of Investigation (FBI). Evidence prints that are not matched with a known person are maintained as evidence in an NYPD computer or case management system, and within AFIS.

The NYPD utilizes 3 different types of digital fingerprint scanning devices and a smartphone application The first device, manufactured by Idemia, is a stationary piece of equipment that allows for digitally scanning a fingerprint and transmitting it for comparison during arrest processing.

Another type of digital fingerprint scanning devices used by the NYPD is a mobile identification device (MID), manufactured by Dataworks+, that is a portable handheld fingerprint scanning device that connects to a small number of NYPD-issued Personal Electronic Devices (PEDs).[1] The MIDs are used to aid in the identification of suspects being issued summonses who do not possess valid identification and voluntarily consent to the scan. Subjects have the right to refuse; however,

[1] For additional information on NYPD-issued Portable Electronic Devices, please refer to the Portable Electronic Device impact and use policy.

an arrest is appropriate if a subject refuses a fingerprint scan in absence of valid identification. A digital fingerprint scan is transmitted for comparison in the same manner as on the stationary equipment. If the subject's fingerprints are in the system, the tablet will provide the subject's information, including any active warrants.

A third device of digital fingerprint scanning devices used by the NYPD is a mobile Livescan device (MLD), manufactured by Dataworks+, which allows for digitally scanning a fingerprint and transmitting it for comparison during arrest processing of hospitalized defendents.

Additionally, certain NYPD personnel assigned to the Detective, Patrol, Transit, and Housing Bureaus have access to a mobile digital fingerprint scanning application, known as "Idemia Morpho Biometric Check," on their NYPD-issued smartphones. This application can be used by officers depending on their specific assignment. The application enables officers to conduct touchless fingerprint scans using their smartphone camera in the field. If the application detects a match, it returns information pertaining to the "matched" individual's identity, including any active warrants for that person. The mobile fingerprint scanning application performs the same function as the physical equipment. However, the fingerprint on the application is only transmitted for comparison within the local NYPD AFIS, not to the state or national AFIS. Fingerprints obtained using the mobile fingerprint application are not saved in the application or locally.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD's digital fingerprint scanning devices must be used by the NYPD 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.

No matter which type of device is being used, NYPD personnel may only use digital fingerprint scanning devices to take fingerprints while executing their lawful duties and the devices may only be used for legitimate law enforcement purposes.

The mobile application may be used in various ways. Detective Bureau personnel may use the application to aid in the identification of deceased and/or unknown persons. Personnel assigned to Patrol, Transit, and Housing Bureaus may use the application to aid in the identification of deceased and/or unknown persons, and to confirm the identity of a person for issuance of a summons in the field.

During arrest processing, NYPD personnel will normally use stationary fingerprint scanning device, unless a bedside arraignment is required. NYPD personnel taking the fingerprints will follow the prompts from the digital fingerprint scanning devices, and scan each finger and thumb of both the left and right hand, along with a palm print of each hand.

Following New York's Criminal Procedure Law, the Family Court Act and the Patrol Guide, fingerprints and palm prints must be taken during the arrest process as indicated below:

1. An adult charged with:
    a. Any felony;
    b. A misdemeanor as defined in the Penal Law;

   c. A misdemeanor defined outside the Penal Law which would constitute a felony if such person was previously convicted of a crime; and
   d. Loitering for purpose of engaging in prostitution

2. An adolescent offender charged with any felony;

3. A juvenile offender charged with a felony listed in Criminal Procedure Law Section 1.20(42); and

4. Other juveniles not classified as adolescent offenders or juvenile offenders, such as:
   a. 12 years of age or older charged with an "A" or "B" felony; and
   b. 13 years of age or older charged with any felony.

NYPD personnel may only conduct fingerprint comparisons for the following reasons:

1. Establish positive identification of persons and for persons arrested for an offense that requires fingerprinting;

2. Collect latent fingerprints from a crime scene; or

3. Process non-criminal fingerprint applicants for employment by the federal, state or other city agencies or in the private sector, for licenses or permits used by federal, state or other city agencies, or other non-criminal purposes.

Consent will be obtained prior to the use of digital fingerprint scanning devices for purposes other than arrest processing, unless an exigency applies, such as attempting to identify a missing person with dementia.

Court Authorization: A court order does not need to be obtained prior to the use of digital fingerprint scanning devices during arrest processing in connection with a variety of arrestable offenses as indicated above. No reasonable expectation of privacy exists in finger and palm prints discovered during a lawful investigation.

Additional Guidelines: Absent arrest processing, digital fingerprint scanning devices are not used for NYPD investigations involving political activity. The Intelligence Division 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 of the individual.

The misuse of digital fingerprints scanning devices 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 digital fingerprint scanning devices.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Physical Safeguards & Security Measures: Digital fingerprint scanning devices are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the equipment. Access to digital fingerprint scanning equipment is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

Data Safeguards & Security Measures: NYPD personnel access to AFIS is limited to authorized users who are authenticated by username and password. Access is limited to NYPD personnel with an articulable need to use AFIS in furtherance of a lawful duty. AFIS access is removed when it is no longer necessary for NYPD personnel to fulfill their duties.

Fingerprint data obtained using NYPD digital fingerprint scanning devices is stored within an appropriate computer or case management system. Only authorized users have access to fingerprint data. As noted above, fingerprints obtained using the Idemia Morpho application are not saved in either the application or locally on the device itself. 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, 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

Information obtained by the use of digital fingerprint scanning devices 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. Information obtained through the use of digital fingerprint scanning devices is stored in an appropriate NYPD computer or case management system. (As noted above, fingerprints obtained using the mobile fingerprint application are not saved either in the application or locally on the device itself).

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. Access rights within NYPD case management and computer systems are further limited based on 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 the classification of a case investigation record. The classification of case investigation records 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 it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Under the New York Criminal Procedure Law, when a criminal action terminates in favor of the accused, digital fingerprint images must be either destroyed or returned to the accused. If a criminal case is sealed, the New York State Unified Court System electronically notifies the NYPD, and the NYPD expunges the associated fingerprint data from the local AFIS. Pursuant to New York's Family Court Act, fingerprint images taken from juvenile delinquents are expunged from the local AFIS.

The misuse of any fingerprint 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 fingerprint data 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.

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information or data collected by the NYPD's use of digital fingerprint scanning devices.

NYPD will turn over any data connected to a criminal case obtained through the use of digital fingerprint scanning devices to the prosecutor with jurisdiction over the matter in accordance with criminal discovery laws. Prosecutors will provide the images to the defendant(s) in accordance with the same criminal discovery laws.

Other law enforcement agencies may request material contained in NYPD case management systems from the NYPD, including digital fingerprints, in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the material or information related to it, to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, the material or information related to it 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 digital fingerprint scanning devices 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 digital fingerprint scanning devices associated software 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 information obtained using NYPD digital fingerprint scanning devices 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 effected 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 officers receive in-person training at the Police Academy on proper operation of digital fingerprint scanning devices and associated equipment. NYPD personnel must operate digital fingerprint scanning devices in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

NYPD personnel conduct internal audits on the local AFIS to ensure fingerprint images connected with sealed criminal cases are expunged from the system.

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).

Supervisors of personnel using digital fingerprint scanning equipment 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.

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.

Access to the mobile fingerprint scanning application is granted by the Deputy Commissioner of Legal Matters. Requests for focused audits of computer terminal 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 associated with digital fingerprint scanning devices. 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 digital fingerprint scanning devices.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that digital fingerprint scanning devices are used effectively and responsibly. Digital fingerprint scanning devices, like all surveillance technologies, have the potential to affect different communities in varied ways. The NYPD does not believe that this technology is being used in a manner that disparately impacts any protected groups as defined in the New York City Human Rights Law.

The safeguards and audit protocols built into this impact and use policy for digital fingerprint scanning devices mitigate the risk of partial and biased law enforcement. Fingerprint matches identified by AFIS are confirmed by NYPD fingerprint technicians. Additionally, digital fingerprint scanning devices do not use any other biometric measurement technologies besides capturing a digital fingerprint image. Based on these safeguards, any theoretical risks of digital fingerprint scanning devices 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.