DIGITAL FINGERPRINT SCANNING DEVICES: IMPACT AND USE POLICY

APRIL 11, 2021

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.

ABSTRACT

Fingerprints are a common biometric measurement inextricably connected to the modern world of policing and law enforcement. The New York City Police Department (NYPD) uses digital fingerprint scanning devices to quickly confirm identification, perform warrant and criminal history background checks and provide police with potential leads in criminal investigations.

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

Fingerprints are a series of friction ridges on the skin of fingertips, sides of fingers and palms of hands. Fingerprint patterns are randomly created during embryonic gestation. Everyone, even identical twins, has their own unique fingerprint. NYPD digital fingerprint scanning devices are inkless, electronic devices capable of recording fingerprints in a digitized format.

Compared to traditional ink fringerprinting methods, use of digital fingerprint scanning devices improves the quality of fingerprint scans and reduces the amount of time required to both scan fingerprints and for the NYPD to receive any associated information. Additionally, digital fingerprint scanning devices allow personnel to efficiently retake a print several times to ensure a quality image is recorded.

The Automated Fingerprint Identification System (AFIS) is a local, state or national database that contains two types of fingerprint records: known finrgerprints 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 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.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD's digital fingerprint scanning device policy seeks to balance the public safety benefits of this technology with individual privacy. 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.

NYPD personnel may only use digital fingerprint scanning devices to take fingerprints while executing their lawful duties and the system may only be used for legitimate law enforcement purposes. 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 engageing 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. 11 years old or older charged with an A or B felony; and
    b. 13 years old or older charged with any felony.

Following the prompts from the digital fingerprint scanning devices, the NYPD personnel taking the fingerprints will scan each finger and thumb of both the left and right hand, along with a palm print of each hand.

NYPD personnel may only conduct fingerprint comparisons to:

1. Establish positive identification of persons and for persons arrested for a fingerprintable offense;
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.

A court order does not need to be obtained prior to use of digital fingerprint scanning devices. The scanning of finger and palm prints in connection to a variety of arrestable offenses is required by New York law. No reasonable expectation of privacy exists in finger and palm prints discovered during a lawful investigation.

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.

NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the *Handschu* Consent Decree.

No person will be the subject of police action solely 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.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

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 devices. Access to digital fingerprint scanning devices is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to digital fingerprint devices is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

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. 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 are 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 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. Members of the NYPD 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 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 information may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Information obtained by the use of digital fingerpring scanning devices are stored in an appropriate NYPD computer or case management system. 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 Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[1] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[2]

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.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years

[1] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[2] *See* NYC Charter 3003.

after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of relevant case investigation record.

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 fingerpint 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 fingerpint 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 law and NYPD policy.

EXTERNAL ENTITIES

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

Other law enforcement agencies may request material contained in NYPD case management systems from the NYPD 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.

Government agencies at the local, state, and federal level, including law enforcement agencies other than the NYPD, have limited access to NYPD computer and case management systems. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases digital fingerprint scanning devices and associated equipment or Software as a Service (SaaS)/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 as soon as practicable. 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 publically 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 devices 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.

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 health and safety issues with digital fingerprint scanning devices or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for digital fingerprint scanning devices mitigate the risk of impartial and biased law enforcement. NYPD fingerprint techniciains confirm a fingerprint match identified by AFIS. Digital fingerprint scanning devices do not use biometric measurement technologies other than the capturing of a digital fingerprint image.

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.