MOBILE X-RAY TECHNOLOGY: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that mobile x-ray technology does not use artificial intelligence and machine learning.	Public comment highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon mobile x-ray technology capabilities.	Added language clarifying mobile x-ray technology capabilities.
Expanded upon mobile x-ray technology rules of use.	Added language clarifying mobile x-ray technology rules of use.
Expanded upon mobile x-ray technology safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to mobile x-ray technology when job duties no longer require access.
Expanded upon mobile x-ray technology data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon mobile x-ray technology external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Expanded upon health and safety language for mobile x-ray technology.	Added language detailing radiation exposure measurements recorded five (5) and ten (10) feet away from the center of the device.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

Government agencies, including law enforcement, use x-ray technology to conduct security screenings. In extremely limited and special circumstances, the New York City Police Department (NYPD) uses mobile x-ray technology to rapidly screen motor vehicles, trucks, temporary enclosed structures and similar objects located on or near a public street for items posing a grave risk to public-safety.

The NYPD produced this impact and use policy because, in the rare event that mobile x-ray is used in the vicinity of a person, the technology will collect a photo-like x-ray image of that person.

CAPABILITIES OF THE TECHNOLOGY

NYPD mobile x-ray technology operates similarly to x-ray screening technologies used by the Transportation Security Administration (TSA) in airports. When the technology is activated, low energy x-rays are emitted from the system and interact with both organic and inorganic matter. NYPD mobile x-ray technologies process the x-rays reflected back to the device to create a photo like x-ray image of concealed objects.

The x-ray image is displayed on a monitor connected to the mobile x-ray device. When appropriate, the generated x-ray images can be retained. The mobile x-ray technology has a limited effective use range. Anything outside of that range will either appear as blurry or not viewable. Generated x-ray images are viewable on a monitor directly wired into the system. NYPD mobile x-ray technology does not contain any wireless, Wi-Fi, streaming, or remote access technologies.

When used, NYPD mobile x-ray technology screens motor vehicles, trucks, temporary enclosed structures, and other objects located on or near a public street for concealed items, objects, or materials posing a grave risk to public-safety. NYPD mobile x-ray technology is used to assist law enforcement in securing physical locations at events with an elevated threat environment. For example, mobile x-ray technology may be used to secure locations during United States Presidential visits or the United Nations General Assembly.

NYPD mobile x-ray technology is not equipped with license plate readers (LPRs)[1]. NYPD mobile x-ray technology does not use facial recognition technologies. NYPD mobile x-ray technology uses x-rays to create an x-ray image and does not use any additional biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD mobile x-ray technology policy seeks to balance the public safety benefits of this technology with individual privacy. Mobile x-ray 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.

NYPD mobile x-ray technology may only be used by NYPD personnel for legitimate law enforcement purposes. Mobile x-ray technology is not and will not to be used to intentionally and knowingly screen people. NYPD personnel are to avoid using the technology in situations where

[1] For additional information on LPRs, please refer to the LPR impact and use policy.

members of the public may be screened. NYPD mobile x-ray technology is not used to screen people, homes, or buildings.

Mobile x-ray technology may be requested by NYPD executives (i.e., uniformed personnel in the rank of Captain or above), as well as external entities (see below for additional information). Final determinations on the use of mobile x-ray technology are made by an executive member of the NYPD Counterterrorism Bureau (CTB) on a case by case basis.

Only members of CTB who have received training in the use and operation of mobile x-ray technology are authorized to use the technology. Members of the CTB executive staff may elect to use mobile x-ray technology if the situation appears appropriate for its use. CTB commanders are responsible to ensure proper usage of mobile x-ray technology.

The NYPD does not seek court authorization for its limited use of mobile x-ray technology. The technology is operated in extremely limited circumstances and comports with the special needs exception to the warrant requirement.

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.

The misuse of mobile x-ray technology will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

NYPD mobile x-ray technology is securely stored by the NYPD in locations when not in use, in a location inaccessible to the public. Additionally, a supervisor must periodically inspect and account for all NYPD mobile x-ray technologies. Access to NYPD mobile x-ray technology is critically limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD mobile x-ray technology 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).

X-ray images relevant to an investigation are retained within an appropriate NYPD computer or case management system. Only authorized users have access to these recordings. 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 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 NYPD mobile x-ray technology software is not capable of reversing, rewinding, or any other kind of playback any of the x-ray images captured.

An x-ray image displayed on the monitor can be downloaded to a local storage system and later uploaded for retention in an NYPD computer or case management system. If an x-ray image is not downloaded, it is automatically overridden on what is known as a first-in-first-out basis; when newly processed x-ray images need to be displayed on the monitor, the oldest x-ray image is automatically deleted to make room for the new x-ray image. Once an image passes through the devices' field-of-view, it cannot be retrieved from the computer system of the mobile x-ray technology.

X-ray images 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. Relevant x-ray images 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 computer and case management 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.[2] 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.[3]

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 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.

The misuse of any x-ray image will subject employees to administrative and potentially criminal penalties.

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

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

Members of the public may request x-ray images created from NYPD use of mobile x-ray 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 law and NYPD policy.

EXTERNAL ENTITIES

External entities may request the assistance of the NYPD and the use of the mobile x-ray technology at a particular location, event, address, etc. The decision whether or not mobile x-ray technology will be used is made at the executive level of CTB. Only members of the NYPD who have received training in the use and operation of mobile x-ray technology will operate the device. Custody and control of the mobile x-ray technology will never be turned over to the external entity.

If mobile x-ray technology obtains an x-ray image relevant to a criminal case, the NYPD will turn the x-ray image over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the x-ray image to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request x-ray images contained in NYPD computer and case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the x-ray image 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, x-ray images relating to mobile x-ray 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; or

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 mobile x-ray technology 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 mobile x-ray technology 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 x-ray images obtained using NYPD mobile x-ray technology are 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 personnel utilizing mobile x-ray technology receive specialized command level training on the proper operation of the technology and associated equipment. NYPD personnel must use mobile x-ray technology in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing mobile x-ray 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

The x-ray levels needed for NYPD mobile x-ray technology to function is measured according to well-established guidelines and procedures established by the American National Standards Institute (ANSI), the European Atomic Energy Community (Euratom), and the International Commission on Radiological Protection (ICRP). The manufacturer ensures compliance with the standards is measured and confirmed by several third-party organizations. The NYPD Radiation Safety Officer also assesses the mobile x-ray technology to ensure the technology is functioning safely.

The level of radiation used by NYPD mobile x-ray technology is no more than the background radiation emitted by natural sources that the average person is exposed to. The exposure to a person directly scanned by the device is similar to exposure received during a short plane flight or by spending a day in the Rocky Mountains. Total exposure at five (5) feet away from the device for ten (10) seconds is between 0.016 mrm (or 16 urem/microrem) and 0.009 mrem (or 3 urem). Total exposure at ten (10) feet away from the device for ten (10) seconds is between 0.004 mrem (or 4 urem) and 0.003 mrem (or 0.3 uR). The health risk to a person exposed to NYPD mobile x-ray technology is considered trivial by the ICRP. There are no anticipated health effects from the low energy x-rays needed for NYPD mobile x-ray technologies to function.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for mobile x-ray technology mitigate the risk of impartial and biased law enforcement. NYPD mobile x-ray technology is used to assist law enforcement in securing physical locations at events with an elevated threat environment. NYPD mobile x-ray technology is not to be used to knowingly screen people. There is no ability to edit or change the x-ray image in anyway. Mobile x-ray technology is disconnected from NYPD databases, cannot scan license plates, and do not utilize any GPS technologies.

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 initiates 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.