AUDIO-ONLY RECORDING DEVICES, COVERT: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that covert audio-only recording 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 covert audio-only recording device capabilities.	Added language clarifying covert audio-only recording device capabilities.
Expanded upon covert audio-only recording device rules of use.	Added language clarifying covert audio-only recording device rules of use.
Expanded upon covert audio-only recording device safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to covert audio-only recording devices when job duties no longer require access.
Expanded upon covert audio-only recording device data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon covert audio-only recording device external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

The New York City Police Department (NYPD) uses covert audio-only recording devices to create objective real-time acoustic recordings, develop investigations, and to protect investigators and informants at risk during sensitive investigations.

The NYPD produced this impact and use policy because covert audio-only recording devices are capable of recording acoustic data, including conversations, occurring within the range of the device which allows the acoustic data to be retained by NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Covert audio-only recording devices are pieces of concealable equipment that can record acoustic (i.e., sound) data. The device is housed in such a way that the identity of the device is not immediately recognizable, is hidden, or is otherwise concealed. Covert audio-only recording devices use a microphone to record any auditory signal that occurs within the devices' recording range, such as: voices, conversations, gunshots, music, etc. NYPD covert audio-only recording devices create a contemporaneous and objective audio record during sensitive law enforcement investigations.

While the majority of the NYPD covert audio-only covert devices are incapable of streaming, a small number of devices are capable of real-time transmission of acoustic data to a remote location. The transmission of this acoustic data promotes the safety of undercover officer(s) involved in investigations.

None of the NYPD covert audio-only recording devices are imbedded with any editing features, and cannot be used to change an audio recording. Covert audio-only recording devices do not use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD covert audio-only recording device policy seeks to balance the public safety benefits of this technology with individual privacy. Covert audio-only recording devices 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.

Covert audio-only recording devices may only be used by NYPD personnel for legitimate law enforcement purposes, and supervisory personnel responsible for oversight must authorize the use. The underlying facts are considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purpose to utilize the technology in a given circumstance.

In most instances, court authorization does not need to be obtained prior to NYPD use of covert audio-only recording devices. Penal Law Sections 250.00 and 250.05 make New York a one—party consent recording state – meaning that a conversation between two or more individuals may be recorded without criminal penalty if at least one of the parties consents to being recorded. Thus, in most instances where the NYPD utilizes a covert audio-only recording device, neither a warrant nor the consent of all parties is required to record a conversation, so long as a member of the NYPD is a participant in the conversation.

A warrant must first be obtained prior to use of covert audio-only recording devices if the queried location maintains a reasonable expectation of privacy. The warrant is obtained with the aid of the prosecutorial agency with proper jurisdiction. The warrant must contain a finding of probable cause by a judge, as well as an explicit authorization for use of a covert audio-only recording device.

Covert audio-only recording devices utilized pursuant to a warrant are used in conjunction with the Communication Assistance for Law Enforcement (CALEA) collection system. The CALEA collection system is the program that allows NYPD investigators to access, review and make use of the recordings created by the covert audio-only recording devices. Only the NYPD Technical Assistance Response Unit (TARU) can deploy and install covert audio-only recording devices utilized pursuant to a warrant. Similarly, only TARU can provide NYPD investigators with access to the CALEA collection system.[1]

Audio-only recording devices utilized pursuant to a warrant will only be deployed for the time period authorized by the warrant obtained by the NYPD investigator. Upon expiration of the court order, use of the audio-only recording device(s) used in connection to that particular investigation is terminated, and the physical device is returned its command.

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 covert audio-only recording 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.

The misuse of covert audio-only recording devices will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Covert audio-only recording 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 covert audio-only recording devices is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to the covert audio-only recording 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).

[1] For additional information on the CALEA collection system, please refer to the CALEA collection system impact and use policy.

Recordings obtained from covert audio-only recording devices 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 NYPD computer and case management systems, 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

Recordings obtained by most NYPD covert audio-only recording devices are stored locally, either within a memory card inserted into the device or to the device itself. Once storage reaches maximum capacity, the device stops recording. The device cannot continue recording until the memory is cleared.

Recordings obtained by covert audio-only recording devices installed by TARU pursuant to a warrant are recorded to the CALEA collection system. Upon conclusion of the investigation, the investigator's access to the CALEA collection system is terminated and data obtained during the

investigation is provided to the NYPD investigator for long-term retention. Recordings are permanently deleted from the CALEA collection system on a first-in-first-out basis; when newly recorded data needs to be stored, it automatically records over the oldest data stored within the CALEA collection system. The data retention period within the CALEA collection system is dependent on restrictions based on storage capacity.

Recordings 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 recordings 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.[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)

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

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 recording 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 recording obtained from NYPD use of covert audio-only recording technology pursuant to 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

If a covert audio-only recording device obtains a recording related to a criminal case, the NYPD will turn the recording over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the recording to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request recordings contained in NYPD case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the recording, 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 recording 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, members of the NYPD 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 or 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 covert audio-only recording 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 covert audio-only recording 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 recordings obtained using NYPD covert audio-only recording devices 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 using covert audio-only recording devices receive command level training on the proper operation of the technology and associated equipment. TARU personnel receive command-level training on the installation and operation of covert audio-only recording devices installed pursuant to a search warrant. Additionally, TARU personnel provide informal training on operation of covert audio-only recording devices and CALEA to NYPD investigators. All NYPD personnel must operate any covert audio-only recording device and any associated equipment in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of a covert audio-only recording device, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing covert audio-only recording 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.

Only TARU personnel can install covert audio-only recording devices and grant NYPD investigators access to the CALEA system. All necessary documentation must be provided to TARU, including the court order authorizing and describing the terms of the installation. A covert audio-only recording device will not be installed if all necessary documentation is not provided by the NYPD investigator to TARU, even in exigent circumstances.

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 health and safety issues with covert audio-only devices or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for covert audio-only recording devices mitigate the risk of impartial and biased law enforcement. NYPD covert audio-only recording devices create contemporaneous and objective audio recordings, and the devices cannot be used to edit or change the recording. NYPD utilization of covert audio-only recording devices does not use any biometric measurement technology.

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.