ABSTRACT

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

The NYPD produced this impact and use policy because covert audiovisual recording devices create recordings containing video images of people, license plates, locations and other visual data, as well as acoustic data occurring within range of the device. The recordings are shared with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Covert audiovisual recording devices are concealable pieces of equipment capable of simultaneously recording acoustic (i.e., sound) data and video images occurring within range of the sensors imbedded into the device. The device is housed in such a way that the identity of the device is not immediately recognizable, or is hidden or otherwise concealed. Covert audiovisual devices capture valuable evidence by creating contemporaneous and objective records during undercover law enforcement operations.

Covert audiovisual recording devices are not connected into any networked camera systems. Most covert audiovisual recording devices for not used real-time observation. However, some NYPD audiovisual recording devices are capable of transmitting audiovisual as well as location data to NYPD personnel observing in a remote location.

None of the NYPD’s covert audiovisual recording devices contain any editing features, and the devices cannot be used to change an audiovisual recording. Covert audiovisual recording devices do not use artificial intelligence, machine learning, video analytics, facial recognition, or any other biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD’s covert audiovisual recording device policy seeks to balance the public safety benefits of this technology with individual privacy. Covert audiovisual 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 audiovisual recording devices are typically used during sensitive law enforcement operations. The underlying facts of each scenario are considered prior to the utilization of the technology, including the safety risks to undercover personnel or informants that may be involved in the operation. NYPD investigators may only use covert audiovisual recording devices to execute their lawful duties, which relate only to official business of the NYPD.
When covert audiovisual recording devices will be used in settings where individuals maintain a reasonable expectation of privacy, the devices are used with court authorization in the form of a warrant. The prosecutor with jurisdiction over the matter assists NYPD personnel with obtaining a warrant. NYPD personnel must use the covert audiovisual recording device in accordance with the terms of that court order. Upon expiration of the court order, use of the audiovisual recording device(s) deployed in connection to that particular investigation is terminated, and the physical device is returned its command.

The NYPD does not seek court authorization prior use when they are used to memorialize locations under exigent circumstances, or locations that do not enjoy a reasonable expectation of privacy.

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 audiovisual 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 audiovisual recording devices will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Covert audiovisual recording equipment is securely stored within NYPD facilities when not in use, in a location inaccessible to the public. The devices are only accessible to personnel needing to utilize the devices to execute their lawful duties. Additionally, a squad supervisor must periodically inspect and account for all covert audiovisual recording devices.

Recordings obtained from overt audiovisual recording devices used for remote streaming may be accessed either on the device itself, or through a private video server located at a NYPD facility. Access to the server is limited to NYPD personnel with a need to access recordings based on a lawful duty. Authorized personnel must be authenticated by a username and password before recordings from the server may be accessed.

Recordings are retained within an NYPD computer or case management system. Only authorized users have access to 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.

DRAFT FOR PUBLIC COMMENT:
POSTED JANUARY 11, 2021
The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. All NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory authentication. The active directory 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 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 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**

Most recordings are stored locally either to the device itself or to a removable memory card inserted into the device. Once the local storage of the device or removable memory card hits max capacity, the device stops recording. The device cannot continue recording until the memory is cleared.

Remotely-streamed audiovisual recordings are stored on a private video server, and is deleted on what is known as a first-in-first-out basis; when newly recorded data needs to be stored, it is automatically recorded over the oldest data currently on the server.

Length of retention varies and depends on size of storage, type of device used to create the recording, amount of movement in field of view, quality of the recordings and similar factors.

Recordings stored within NYPD computer and case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. 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.

The misuse of any recordings 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 recordings obtained from NYPD use of covert audiovisual recording devices 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

If a covert audiovisual recording device obtains a recording relevant 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 computer or 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;
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 covert audiovisual 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 audiovisual 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.

**TRAINING**

NYPD personnel using covert audiovisual recording devices receive command level training on the proper operation of the technology and associated equipment. NYPD personnel must operate covert audiovisual recording devices in compliance with NYPD policies and training.

**INTERNAL AUDIT & OVERSIGHT MECHANISMS**

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

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 recordings 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 audiovisual recording 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. Covert audiovisual recording devices only record audio and visual information occurring within the close proximity to the device. Covert audiovisual recording devices do not use artificial intelligence, machine learning, or any other biometric measurement 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 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.