



**AUDIOVISUAL RECORDING DEVICES, COVERT:
IMPACT AND USE POLICY**

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that covert audiovisual 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 audiovisual recording device capabilities.	Added language clarifying covert audiovisual recording device capabilities. Added language describing how covert audiovisual recording devices compliment other NYPD technologies.
Expanded upon covert audiovisual recording device rules of use.	Added language clarifying covert audiovisual recording device rules of use.
Expanded upon court authorization language for covert audiovisual recording devices.	Added language clarifying what needs to be demonstrated during an application for court authorization.
Expanded upon covert audiovisual recording device safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to covert audiovisual recording devices when job duties no longer require access.
Expanded upon covert audiovisual recording device data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon covert audiovisual recording device external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

AUDIOVISUAL RECORDING DEVICES, COVERT REVISION

Date of Revision	Description of Revision
February 4, 2026	This impact and use policy was revised to comply with the recently passed amendment to the POST Act under Local Law 56 of 2025.

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.

NYPD covert audiovisual recording devices are not connected into any networked camera systems. Most covert audiovisual recording devices are not used for 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. Personal use of this technology is prohibited.

NYPD covert audiovisual recording devices do not contain any editing features, and the devices cannot be used to change an audiovisual recording. Covert audiovisual recording devices do not use video analytics or any biometric measuring technologies like facial recognition analysis.¹

The manufacturers' names have been intentionally withheld to protect the safety of undercover officers utilizing these devices in the course of their official duties. Providing the manufacturer potentially allows bad actors to inquire how the manufacturer may disguise devices and allow for identification, placing an undercover officers' lives and safety at significant risk.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD's 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 may only be used by NYPD personnel for legitimate law enforcement purposes or other official business of the NYPD. The 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

¹ However, a still image can be created from the recorded video images and may be used as a probe image for facial recognition analysis. For additional information on facial recognition, please refer to the facial recognition impact and use policy.

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.

Court Authorization: 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.² The prosecutor with jurisdiction over the matter assists NYPD personnel with obtaining the warrant, and the warrant application must be made under oath.

For a judge to grant the warrant, the judge must find: 1) there is probable cause to believe a person is committing, has committed, or is about to commit a designated offense;³ 2) there is probable cause to believe particular observations concerning the offense will be made; and 3) normal investigative procedures have been tried and failed, are unlikely to succeed if tried, or too dangerous to employ. The warrant cannot allow the use of the NYPD covert audiovisual recording devices for any period longer than necessary; a maximum of 30 days. The NYPD investigator and prosecutor can apply to the judge for an extension of the warrant, and the judge must make similar findings to the original application to extend it.

The NYPD does not seek court authorization prior to using covert audiovisual recording devices when they are used in locations that do not enjoy a reasonable expectation of privacy or under exigent circumstances.

In order to use covert audiovisual recording devices in exigent circumstances without first obtaining a warrant, an NYPD investigator must have probable cause to believe: 1) a person is committing, has committed, or is about to commit a designated offense;⁴ (2) an emergency exists as result of the criminal conduct; (3) there is an immediate urgent need for assistance due to an imminent danger of serious bodily injury or death to any person making it impracticable to prepare a written application without such risk occurring; *and* (4) the effort to locate a suspect is being undertaken with the primary concern of preventing serious injury or death and is not primarily motivated by an intent to arrest and seize evidence. The possibility of flight of a suspect does not on its own constitute an exigent circumstance. An emergency warrant must be subsequently obtained and cannot be extended.

Additional Guidelines: If necessary, the Intelligence Division will determine the need for covert audiovisual recording devices for NYPD investigations involving political activity. The Intelligence Division is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Revised *Handschu* Guidelines.

As with all NYPD operations, no person will be the subject of police action because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender

² For a New York State investigation, the application is for a video surveillance warrant. If the NYPD is assisting with a federal investigation, the application is for a search warrant.

³ New York designated offenses are defined by N.Y. Crim. Proc. Law § 700.05(8). If the NYPD is assisting with a federal investigation, an application for a search warrant can be made in connection to any ongoing federal criminal investigation.

⁴ Please see definition above.

(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.

Addendum Obligation: In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of covert audiovisual recording devices.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

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

Data Safeguards & Security Measures: Recordings obtained from covert audiovisual recording devices are retained locally, either within a memory card inserted into the device or to the device itself. Only authorized users have access to these recordings. Recordings may be downloaded and retained within the NYPD case management system. 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. NYPD personnel utilizing computer and case management systems are authenticated by username and password.

Devices used for remote streaming may be accessed either on the device itself, or through a private video server located at a NYPD facility. Data is encrypted both at rest on the device and in transit. 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. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case-by-case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with 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 from unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA

Recordings obtained by NYPD covert audiovisual recording devices may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigation, and disciplinary proceedings. Recordings obtained by most NYPD covert audiovisual recording devices 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 reaches its maximum 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 are deleted on a first-in-first-out basis, meaning that 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 other similar factors.

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 NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. The retention period of a “case investigation record” depends on its classification and 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

they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought..

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 data collected by the NYPD through its 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 the law.

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by covert audiovisual devices.

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; 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.

Vendors & Contractors: The NYPD purchases covert audiovisual recording devices and associated equipment or software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD 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.

If recordings obtained using NYPD covert audiovisual 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 within 24 hours. The NYPD must make reasonable efforts to notify individuals affected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publicly available online.

TRAINING

NYPD 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 audiovisual 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.

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 tests or reports regarding the health and safety effects of covert audiovisual recording devices. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of covert audiovisual recording devices or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure the covert audiovisual recording devices are used effectively and responsibly. The NYPD does not believe that this technology has shown any potentially disparate impacts on any protected groups as defined in the New York City Human Rights Law.

The safeguards and audit protocols built into this impact and use policy for covert audiovisual recording devices mitigate the risk of partial and biased law enforcement. Covert audiovisual recording devices only record audio and visual information occurring within the close proximity to the device. These devices are only deployed for investigative purposes under supervisory review. The NYPD restricts access to authorized personnel only. Covert audiovisual recording devices do not use biometric measurement technologies. Based on these safeguards, any theoretical risks of covert audiovisual recording devices disparately impacting protected groups are effectively mitigated.

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.