CLOSED CIRCUIT TELEVISION SYSTEMS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that CCTV systems 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 CCTV system capabilities.	Added language clarifying CCTV system capabilities. Added language describing how CCTV systems compliment other NYPD technologies.
Expanded upon CCTV system rules of use.	Added language clarifying CCTV system rules of use.
Expanded upon CCTV system safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to CCTV systems when job duties no longer require access.
Expanded upon CCTV system data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon CCTV system 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 Closed-Circuit Television (CCTV) systems as a cost-effective tool to help NYPD personnel obtain real-time and/or recorded visual information, aid in crime deterrence, reduce incident response times, provide archived video coverage for investigations and criminal prosecutions, enhance public and officer safety, and provide infrastructure security.

The NYPD produced this impact and use policy because CCTV systems have the ability to record video images of people and other visual information within range of the cameras, and share video images with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Security-video-systems typically exist on the same network and consist of analog and/or internet protocol (IP) cameras within the same network. Those networks can consist of closed-circuit video cameras that captures video-only feeds or a stand-alone system with one video-only camera monitoring a specific area. NYPD personnel can access CCTV systems that are owned by the NYPD or owned by external entities. External entities must provide the NYPD with access rights to the system before NYPD personnel can view the CCTV video.

NYPD CCTV cameras capture only capture video images and are incapable of capturing acoustic data. The CCTV cameras the NYPD uses or accesses consist of both fixed cameras and pan-tilt-zoom (PTZ) cameras.

PTZ cameras allows officers monitoring or reviewing the footage to direct attention to a specific location by allowing users to move the field of view horizontally (pan), vertically (tilt) or to magnify it (zoom). Other cameras are set to automatically adjust their recording range on a set schedule. NYPD CCTV cameras contain low-light technology to support detection of unauthorized or suspicious activities at night.

NYPD Detectives, Sergeants, and higher ranked members can access live video from CCTV systems either: 1) by using the NYPD Domain Awareness System (DAS) [1] at an NYPD desktop, or 2) through an app on an NYPD issued portable electronic device (PED). [2]

NYPD personnel use CCTV video to further investigations by linking data elements, and aiding in the identification of individuals. Under these circumstances, the NYPD may use an image, such as a license plate number, captured by the video feed to identify an individual or vehicle or link an individual or vehicle to a specific event or investigation.

NYPD CCTV cameras and systems do not use video analytics or any other biometric measurement technologies. NYPD CCTV cameras do not use facial recognition technologies and cannot conduct a facial recognition analysis. However, a still image can be created from a CCTV video image and may be used as a probe image for facial recognition analysis.[3]

[1] For additional information on DAS, please refer to the DAS impact and use policy.
[2] For additional information on PEDs, please refer to the PED impact and use policy.
[3] For additional information on facial recognition, please refer to the facial recognition impact and use policy.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD CCTV system policy seeks to balance the public safety benefits of this technology with individual privacy. CCTV systems 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 CCTV systems may only be used by authorized NYPD personnel for legitimate law enforcement purposes. NYPD CCTV camera access for Detectives and Sergeants is limited to the cameras located within their geographical area of employment. Because they frequently work in different commands, NYPD personnel with the rank of Lieutenant or higher have city-wide CCTV system access. Additional NYPD personnel may be granted access to view live video feed from NYPD CCTV systems based on assignment needs. Access must be requested by a Commanding Officer and approved by the NYPD Information Technology Bureau (ITB).

CCTV cameras are only installed by the NYPD to monitor areas that are open and accessible to the public. Similarly, the NYPD will only agree to access an external entity's CCTV cameras that monitor areas that are open and accessible to the public. The field-of-view of all CCTV cameras accessible to NYPD personnel is strictly limited to public areas and locations. Accordingly, court authorization is not necessary in order for the NYPD to use CCTV systems.

The NYPD does engage in cooperative agreements with external entities that have installed their own CCTV cameras in order to share such footage with the NYPD. These entities, which include members of the public and private sectors, may only access video from their own CCTV cameras. External entities cannot access video from CCTV cameras owned by NYPD or from other external entities.

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 use of CCTV systems.

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 CCTV systems will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Access to the physical location where the CCTV footage is digitally stored during the retention period is limited to NYPD personnel, authorized invited guests, and external stakeholders. Physical security protections include: guards, access logs, and locked facilities requiring badges or access cards for entry. All external stakeholders must be screened and authorized by the NYPD.

The ability to review CCTV video in real-time is confidential-password-protected and access is restricted to only authorized users. NYPD personnel authorized to view live CCTV system video consist only of NYPD personnel in various commands, whose access has been requested by their Commanding Officer, and approved by ITB. NYPD CCTV system access is adjusted or removed when the access is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command).

CCTV recordings are retained within a NYPD computer or case management systems. NYPD personnel utilizing NYPD computer and case management 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 to any system will subject authorized users to administrative and potentially criminal penalties.

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

Only authorized users have access to live-video, and all users must abide by NYPD policy and Public Security Guidelines (the Guidelines) while accessing it. The Guidelines list the specific uses for the system and notices use of the system is audited through logs. All external entities must be briefed on the Guidelines and sign an agreement promising to abide by the Guidelines. Sanctions are imposed for any external stakeholder violation.

CCTV systems consist of Network Video Recorders (NVRs) which use hard drives to store recorded video. NYPD policy is to retain CCTV video for thirty (30) days. The devices automatically overwrite previously recorded video with the most recent images unless video has been identified to be retained for security purposes or for criminal investigations. Only members of the Lower Manhattan Security Initiative (LMSI) can download video recorded by a NYPD CCTV system for retention.

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 within 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.[4] 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.[5]

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.

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

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 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 recordings from NYPD CCTV systems 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

Stakeholders that provide the NYPD with access to their own public-space facing cameras have the ability to designate one of their own employees as their stakeholder representative. The stakeholder representative is non-NYPD personnel, and is granted access to the Lower Manhattan Security Coordination Center (LMSCC).

Inside the confines of the LMSCC, the stakeholder representative is only able to view the feed of the cameras that belong to the stakeholder by whom they are employed. The stakeholder representative is not given access to any NYPD-owned cameras, nor any cameras owned by private entities or NYC agencies. Stakeholder representatives must agree to NYPD confidentiality and privacy guidelines. Stakeholders and stakeholder representatives are informed that use of NYPD computer systems beyond authorized access, or for personal or non-NYPD business matters is

strictly prohibited. Stakeholder representatives who are found in violation of this policy are notified that they will be subject to a termination of assignment.

If a NYPD CCTV camera records video related to a criminal case and the recording is requested for retention, the NYPD will turn the recording over to the prosecutor with jurisdiction over the matter. The prosecutor 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 and regulations, 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 the news media, community stakeholders, and others 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 CCTV systems 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 CCTV systems 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 CCTV systems 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 and external stakeholder representatives using NYPD CCTV systems receive command level training on the proper operation of the technology and its associated equipment. NYPD personnel and external stakeholder representatives must use CCTV systems in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Only authorized users are allowed to access live CCTV video, and immutable audit logs are created when any information is searched or accessed. The log-in and use of the system is traceable to a particular user and periodically audited for misuse by the precinct or unit's Commanding Officer.

The Guidelines users must follow while accessing NYPD CCTV systems enumerate the specific uses for the system. The misuse of any system will subject employees to administrative and potentially criminal penalties.

CCTV system access through DAS or the mobile application is auditable by ITB.

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

There are no known health and safety issues with devices or equipment used for CCTV systems or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD CCTV systems mitigate the risk of impartial and biased law enforcement. The CCTV systems accessible by NYPD personnel only monitor areas open and available to the public. CCTV systems do not use video analytics or 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. When an officer's decision to initiate enforcement action against a person is 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 just race, age, and gender, but other identifying characteristics or information.