VEHICLE MOUNTED CAMERAS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that vehicle mounted cameras 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 vehicle mounted cameras capabilities.	Added language describing how vehicle mounted cameras compliments other NYPD technologies.
Expanded upon rules of use.	Added language clarifying vehicle mounted cameras rules of use.
Expanded upon vehicle mounted cameras safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to the technology when job duties no longer require access.
Expanded upon vehicle mounted camera data retention.	Added language to reflect NYPD obligations under federal, state and local record retention laws.
Expanded upon vehicle mounted camera external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

The New York City Police Department (NYPD) uses vehicle-mounted cameras throughout the NYPD's fleet of motor vehicles. Vehicle-mounted cameras support public and officer safety and are used to contemporaneously create an objective recording of law enforcement encounters, provide archived videos for investigations and criminal prosecutions, improve training techniques, foster accountability, and encourage lawful and respectful interactions between the public and the police.

The NYPD produced this impact and use policy because vehicle mounted cameras can capture images of people, vehicles, locations, license plates, any other visual information, and in acoustic data, that occurs within range of the device, and share the data with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Vehicle mounted cameras are video recording devices connected to NYPD vehicles for the purpose of creating a real-time objective record of law enforcement encounters and NYPD trainings.

The NYPD uses three (3) kinds of vehicle mounted cameras:

1. Dashboard Cameras (dash-cams);
2. Transport Cameras; and
3. Watercraft Cameras.

Dashboard Cameras (dash-cams) are cameras that are usually mounted on the dashboard or the windshield of a vehicle. NYPD dash-cams record video of what occurs in front of the vehicle and are capable of recording both video and audio. NYPD dash-cams are installed on both marked and unmarked NYPD vehicles. Once a vehicle is started, NYPD dash-cams continuously record video, re-writing over recorded video in sixty (60) second intervals unless long-term recording is activated. This process is commonly referred to as "buffering." Long-term recording automatically begins when NYPD personnel activates a NYPD's vehicles turret lights. When an officer activates long-term recording, the preceding sixty (60) seconds of video is automatically saved. Those sixty-seconds of recorded video will not contain audio. Once long-term recording is activated, dash-cams record all audio and video data until long-term recording is deactivated. Once deactivated, the dash-cam returns to the buffering state. This process is repeated until the vehicle is returned to its command.

Transport cameras memorialize what occurs within the passenger cabin of a NYPD vehicle during transport of an arrestee. Most devices only record video, however, several transport cameras can record both video images and acoustic (i.e., sound) data.

Watercraft cameras are mounted to several NYPD watercraft used by the Harbor Unit. They record video images of what occurs on the deck or in front of the watercraft. Watercraft cameras do not record any acoustic data.

NYPD vehicle mounted cameras do not contain any editing features, and the devices cannot be used to change recorded data. NYPD vehicle mounted cameras do not use any biometric technologies. NYPD vehicle mounted cameras do not use facial recognition technologies and

cannot conduct facial recognition analysis. However, a still image can be created from the recorded video images and may be used as a probe image for facial recognition analysis.[1]

Additionally, both the NYPD's manned aircraft[2] and unmanned aircraft[3] systems are capable of recording video. However, those technologies differ from the devices covered in this impact and use policy in several ways and have been addressed in independent impact and use policies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD's vehicle mounted camera policy seeks to balance the public safety benefits of this technology with individual privacy. Vehicle mounted cameras 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 vehicle mounted cameras may only be used by NYPD personnel for legitimate law enforcement purposes.

NYPD personnel operating vehicles equipped with dash-cams must activate long-term recording any time a vehicle stop is conducted. Any events for which recording is required must be recorded from start to finish.

NYPD personnel operating any vehicles equipped with a transport camera must activate the camera any time a subject enters the passenger cabin of an NYPD vehicle. Any events for which recording is required must be recorded from start to finish.

Watercraft cameras are used by the NYPD's Harbor Unit to record crew and deck operations performed on NYPD watercraft. NYPD personnel operating watercraft equipped with watercraft cameras must activate the camera when a job is assigned. Any events for which recording is required must be recorded from start to finish.

Access to vehicle mounted cameras is limited to authorized operators of NYPD vehicles equipped with the technology. Vehicle mounted cameras only record what is occurring in real time and include an immutable timestamp. Prior to use of vehicle mounted cameras, the operator must check that the date and time on the device is correct.

The NYPD does not seek court authorization to use vehicle mounted cameras. The devices only record law enforcement encounters occurring in locations that do not maintain 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 use of vehicle mounted cameras.

[1] For additional information on facial recognition, please refer to the facial recognition impact and use policy.
[2] For additional information on the NYPD's manned aircraft systems, please refer to the manned aircraft systems impact and use policy.
[3] For additional information on the NYPD's unmanned aircraft systems, please refer to the unmanned aircraft systems impact and use policy.

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 vehicle mounted cameras will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Vehicles equipped with vehicle mounted cameras are securely stored in NYPD facilities when not in use, in locations inaccessible to the general public. Additionally, a supervisor must periodically inspect and account for all NYPD vehicles equipped with vehicle mounted cameras. Access to vehicle mounted cameras is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD vehicle mounted cameras 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).

Recordings obtained from NYPD vehicle mounted cameras are retained within an NYPD computer or case management system. Only authorized users have access to these recordings. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

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

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

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

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

While powered, NYPD dash-cams continuously record video; re-writing over previously captured video in sixty second intervals unless long-term recording is activated. Long-term recording of dash-cam video is automatically activated when NYPD personnel activates a vehicle's turret lights. The preceding sixty-seconds of recorded video is automatically saved, but will not contain audio. Once long-term recording is activated, the dash-cam records all audio and video until long-term recording is deactivated. Once long-term recording is deactivated, the dash-cam returns to continuously recording video, re-writing over previously captured video in sixty second intervals until long-term recording is activated once again. This cycle continues until the vehicle is returned to its command.

Some NYPD dash-cams store recorded data locally within a removable memory card. Once the memory card reaches maximum capacity, the device stops recording. The device cannot continue recording until the data stored on the memory card is removed. Recordings relevant to a case or investigation will be stored in an appropriate NYPD computer or case management system.

Additionally, some NYPD dash-cams can upload recorded data automatically to a cloud-based storage system when the vehicle is returned to its command. Recordings are uploaded over a secured wireless network to a cloud-based storage system. Authorized users can download recordings from the cloud-based storage system. Once uploaded, the data is removed from the internal memory of the device. Additionally, at the request of a commanding officer, these newer vehicles can upload critical dash-cam recorded data over a cellular network.

Some NYPD transport cameras store recorded data locally within a removable memory card. Once the memory card reaches maximum capacity, the device stops recording. The device cannot continue recording until the data stored on the memory card is removed. Recordings relevant to a case or investigation will be stored in an appropriate NYPD computer or case management system.

Additionally, some NYPD transport cameras can upload recorded data automatically to a cloud-based storage system when the vehicle is returned to its command. Recordings are uploaded over a secured wireless network to a cloud-based storage system. Authorized users can download recordings from the cloud-based storage system. Once uploaded, the data is removed from the internal memory of the device.

All dash-cam and transport camera recordings uploaded to the cloud-based storage system must be assigned a category by NYPD personnel. The category assignment mirrors the retention period for the BWC-recorded video(s) in the cloud-based storage system. The possible category assignment and its associated retention period are as follows:

1. Car Stop, Summons Served	Eighteen (18) Months
2. Car Stop, Arrest Made	Five (5) Years
3. Transport Recording	One (1) Year
4. Turret Light Activation	One (1) Year
5. Vehicle Speed Exceeds Ninety (90) miles per hour	One (1) Year

Data recorded by watercraft cameras is stored locally, within the device itself. Once the local storage of these devices reaches maximum capacity, the device stops recording. The device cannot continue recording until the data stored on the memory card is removed. Data on the memory card can be transferred from the memory card and loaded into an appropriate NYPD computer or case management system.

NYPD transportation camera 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. Recordings relevant to an investigation are retained 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 computer and case management systems are further limited based on lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[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.

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

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

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 recording obtained from NYPD use of vehicle mounted cameras 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 vehicle mounted camera 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 from the NYPD in accordance with applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide retained recordings 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, recordings, 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, 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 vehicle mounted cameras 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 vehicle mounted cameras 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 vehicle mounted cameras 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 assigned to the NYPD Highway Unit receive training in the technical use of dash-cams and the associated equipment. NYPD personnel who have access to vehicle mounted cameras receive command level training on the proper operation of the technology. Officers must operate all vehicle mounted cameras in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

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 the 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 vehicle mounted cameras or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into the impact and use policy for vehicle-mounted cameras mitigate the risk of impartial and biased law enforcement. Vehicle-mounted cameras only record what occurs within the cameras' field-of-view. Vehicle mounted cameras do not use any 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.