SITUATIONAL AWARENESS CAMERAS: IMPACT AND USE POLICY

Updated December 07, 2023

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that situational awareness cameras do not use artificial intelligence and machine learning.	Public comment highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon situational awareness cameras rules of use.	Added additional language clarifying situational awareness cameras rules of use. Added language to clarify situational awareness cameras rules of use-authorization.
Expanded upon safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to situational awareness cameras when job duties no longer require access.
Minor grammar changes.	Minor syntax edits were made.

SITUATIONAL AWARENESS CAMERAS ADDENDUM

Date of Addendum	Description of Addendum
April 11, 2023	NYPD is utilizing an autonomous security robot during a seven-month pilot program.
December 07, 2023	Clarified information related to the autonomous security robot sensor capabilities. Updated policy regarding deployment authorizations.

ABSTRACT

Situational awareness cameras enable New York City Police Department (NYPD) personnel to assess potentially dangerous situations from a safe location. The NYPD produced this impact and use policy because situational awareness cameras are capable of processing both acoustic data and video images, and sharing it with NYPD personnel conducting observation on remote monitors.

CAPABILITIES OF THE TECHNOLOGY

Situational awareness cameras are portable cameras that enable NYPD personnel to observe inside barricaded, hazardous, or otherwise compromised locations from a safe location. The use of situational awareness cameras allows NYPD personnel to gather critical information about a queried location before entry, providing additional safety and security to NYPD personnel, the subjects of the observation, and other members of the community in potentially dangerous situations. The use of an autonomous security robot will provide additional public safety resources and help deter crime.

The NYPD uses five (5) types of situational awareness cameras:

1. Cameras attached to remote-controlled robots;
2. Cameras attached to autonomous security robots travelling along pre-programmed routes;
3. Cameras attached to poles or other extenders;
4. Cameras that can be thrown; and,
5. Handheld scope cameras.

Most NYPD situational awareness cameras only process video images. Some situational awareness cameras can simultaneously process video images and acoustic data (i.e., sound). Select situational awareness cameras, such as the 'Digidog' and autonomous security robot, are capable of transmitting video images, acoustic data, and enable two-way communication between NYPD personnel and any individual near the device. The autonomous security robot uses thermal imaging sensors to alert NYPD personnel of dangerously high temperatures.[1]

Situational awareness cameras send video and, if capable, acoustic data to NYPD personnel reviewing the transmission on a remote monitor through either an encrypted signal, secure data transmission to or from a cloud, or through a direct wired connection between the situational awareness camera and the monitor. Except for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras. The autonomous security robot video will be retained for thirty (30) days.

Depending on the type of device being used, the situational awareness camera may be lowered or thrown into position, attached to a hand-held pole and extended around a corner, maneuvered by a remote control, or operate autonomously along a pre-programmed route. The autonomous security robot uses sensors based on light, sound, orientation, video, and GPS to avoid colliding with anything that may be located on its route. The information from the sensors is solely used by the autonomous robot for object avoidance.

[1] For additional information on thermal imaging sensors, please refer to the Thermographic Cameras impact and use policy.

NYPD situational awareness cameras do not utilize video analytics, facial recognition, or any other biometric measuring technologies, except to the extent that the autonomous security robot uses thermal imaging sensors to alert NYPD personnel of dangerously high temperatures and uses video-based sensors as part of its object avoidance system.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD situational awareness camera policy seeks to balance the public safety benefits of this technology with individual privacy. Situational awareness 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.

Only members of NYPD Emergency Services Unit (ESU) or Technical Assistance Response Unit (TARU) are authorized to use situational cameras and personnel must be trained in their use and appropriate application. A request for use of a situational awareness camera must be made to ESU or TARU and the use request must be approved by a supervisor before the device will be used. NYPD supervisors may elect to use the cameras if the situation appears appropriate for its use. Use of Digidog can only be authorized by the Chief of Department. NYPD situational awareness cameras may only be used by NYPD personnel for legitimate law enforcement purposes. Commanding officers are responsible for ensuring proper usage of situational awareness cameras and accompanying monitors.

NYPD situational awareness cameras cannot be used for routine foot patrol by officers, traffic enforcement, or immobilizing a vehicle or suspect.

The NYPD does not seek court authorization before using situational awareness cameras. Except for the autonomous security robot, NYPD situational awareness cameras are only used during exigent circumstances or in emergency environments. The autonomous security robot will be used to provide additional public safety resources and help deter crime.

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.

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 situational awareness cameras.

As with all NYPD operations, no person will be 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 situational awareness cameras will subject employees to administrative and potentially criminal penalties.

SAFEGUARDS & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Situational awareness cameras 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 the devices. Access to situational awareness cameras is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD situational awareness 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).

NYPD situational awareness cameras transmit video images, and acoustic data if capable, to NYPD personnel reviewing the transmission on a remote monitor through either an encrypted signal on a secured stand-alone network, or through a direct-wired connection between the situational awareness camera and the monitor.

The misuse of any system will subject employees to administrative and potentially criminal penalties.

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

Except for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras. The autonomous security robot data will be retained for thirty (30) days. Situational awareness cameras do not use video analytics, facial recognition, or any other biometric measuring technologies.

Data obtained using situational awareness cameras 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. Data relevant to an investigation are stored in an appropriate NYPD computer or case management system. The data may only be used for legitimate law enforcement purposes. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management 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.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[2] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[3]

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

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) 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 data 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 information related to the NYPD's use of situational awareness camera technology 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

Except for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras.

If the autonomous security robot captures data related to a criminal case, the NYPD will turn it over to the prosecutorial entity with jurisdiction over the matter. Prosecutors will provide the data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request data 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 data 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, information 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;
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 situational awareness 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 autonomous security robot 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 data obtained using the autonomous security robot is 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 utilizing situational awareness cameras receive command level training on the proper operation of the technology and associated equipment. NYPD personnel must operate situational awareness cameras in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Only members of the NYPD ESU or TARU are authorized to use situational cameras. ESU and TARU personnel are specifically trained in their use and in appropriate application of the cameras. Use of situational awareness cameras is a strategic decision made by ESU or TARU personnel during law-enforcement encounters where ESU or TARU responds to requests for assistance. The autonomous security robot will be used to provide additional public safety resources and help deter crime.

Supervisors of personnel utilizing situational awareness cameras are responsible for security and proper utilization of the technology and associated equipment.

HEALTH & SAFETY REPORTING

There are no known health and safety issues associated with the use of situational awareness cameras or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD situational awareness cameras mitigate the risk of impartial and biased law enforcement. Use of situational awareness cameras is a strategic decision made by NYPD executives during law enforcement encounters in which ESU or TARU responds to requests for assistance. Use of the Digidog situational awareness camera can only be authorized by the Chief of Department. Except for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by situational awareness cameras. The autonomous security robot video will be retained for thirty (30) days.

NYPD situational awareness cameras do not utilize video analytics, facial recognition, or any other biometric measuring technologies, except to the extent that the autonomous security robot uses thermal imaging sensors to alert NYPD personnel of dangerously high temperatures and uses video-based sensors as part of its object avoidance system.

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.