THERMOGRAPHIC CAMERAS: IMPACT AND USE POLICY

Updated April 11, 2023

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that thermographic 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 thermographic cameras rules of use.	Added language clarifying thermographic cameras rules of use.
Expanded upon thermographic cameras safeguards and security measures.	Added language regarding information security. Added language to reflect removal of access to the technology when job duties no longer require access.
Minor grammar changes.	Minor syntax edits were made.

THERMOGRAPHIC CAMERAS ADDENDUM

Date of Addendum	Description of Addendum
April 11, 2023	NYPD is utilizing an autonomous security robot during a six-month pilot program that is capable of transmitting infrared thermal images.

ABSTRACT

Thermographic cameras are used by law enforcement personnel to create images using thermal light, i.e. heat, as opposed to a traditional camera that uses visible light. These specialized cameras enhance visibility during operations such as securing large-scale events, search and rescue, hostage negotiation and/or barricaded individuals and other operations conducted in low-visibility environments. The New York City Police Department (NYPD) uses thermographic cameras to enhance NYPD operations by providing real-time observation of the live or residual heat signature of a person or object.

The NYPD produced this impact and use policy because thermographic cameras have the ability to process thermal data of both people and objects, and share a heat signature video image with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

The NYPD utilizes two (2) types of thermographic cameras:

1. Thermal Imaging Cameras; and
2. Infrared Cameras.

All objects, both organic and inorganic, omit infrared light. Infrared light is a type of electromagnetic radiation invisible to the human eye, but it can be felt by humans as heat. Both thermal imaging cameras and infrared cameras measure temperature by capturing different wave frequencies of infrared light being omitted from an object. The cameras process the differences in the measured infrared light, and creates a heat signature video image.

Thermographic cameras allow officers to observe obscured or hazardous containing conditions preventing traditional observation such as darkness, smoke or gas. Thermographic cameras allow for rapid detection of people during a search of a large outdoor location, crime scene monitoring and large-scale disasters. Thermographic cameras are also used during large-scale events to detect heat signature anomalies and during hostage scenarios where officers cannot safely gain access to a location.

Some NYPD handheld thermographic cameras transmit heat signature video images to a monitor directly wired to the device. Others are capable of wireless transmission of heat signature video images to a remote monitor. The NYPD is utilizing an autonomous security robot during a six-month pilot program that is capable of transmitting infrared thermal images. Except for the autonomous security robot, NYPD thermographic cameras do not record, store, or retain any heat signature video images or temperature data.[1]

Thermographic cameras can only process temperature data to create heat signature video images. Thermographic cameras do not use facial recognition technologies and are not capable of conducting facial recognition analysis. Other than the processing of the infrared light emitted by a person or object, the devices do not contain biometric measuring capabilities.

[1] For additional information on the autonomous security robot, please refer to the Situational Awareness Cameras impact and use policy.

Both the NYPD's manned[2] and unmanned[3] aircraft systems are equipped with thermographic cameras. However, the thermographic cameras equipped to manned and unmanned aircraft systems are integrated into a more intricate system. Those systems are each addressed in individual impact and use policies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD thermographic camera policy seeks to balance the public safety benefits of this technology with individual privacy. Thermographic 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 thermographic cameras may only be used for legitimate law enforcement purposes, and supervisory personnel responsible oversight must authorize use. The underlying facts of each investigation are considered prior to the utilization of the technology, including the safety risks to NYPD personnel, civilians and suspects that may be involved in the operation, as well as the legitimate law enforcement purpose to utilize the technology in a given circumstance.

The NYPD does not seek court authorization prior to use of thermographic cameras. The devices are strictly used during emergencies where exigent circumstances exist or to conduct surveillance of locations exposed to public observation.

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 thermographic cameras.

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 thermographic cameras will subject employees to administrative and potentially criminal penalties.

SAFEGUARDS & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Thermographic cameras are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. A supervisor must periodically inspect and account for the equipment. Access to NYPD thermographic cameras is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access 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).

[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.

NYPD thermographic cameras capable of wireless remote viewing transmit thermal images and associated data to a remote monitor over an encrypted signal. NYPD handheld thermographic cameras transmit processed images to a monitor through a direct-wired connection.

Unauthorized access 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 heat signature video images or temperature data processed through the use thermographic cameras. The autonomous security robot data will be retained for thirty (30) days.

Data obtained using the autonomous security robot 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.[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 destroyed), must be retained permanently. Case investigation records classified as a fourth degree

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

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 thermographic 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

Except for the autonomous security robot, the NYPD does not record, store, or retain any of the video or acoustic data processed by thermographic 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 thermographic 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 using thermographic cameras receive command level training on the operation of thermographic cameras and associated equipment. Officers must operate thermographic cameras in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The NYPD's use of thermographic cameras is determined by supervisory personnel responsible for the conduct of a given operation. The autonomous security robot will be used to provide additional public safety resources and help deter crime. Supervisors of personnel utilizing thermographic cameras are responsible for security and proper utilization of the technology and associated equipment.

All members of the NYPD, including those utilizing thermographic cameras, are advised that all NYPD equipment is intended for the purposes of conducting official business. Use of NYPD equipment for personal or non-NYPD business matters is strictly prohibited and individuals who are found in violation of this policy are notified that they will be subject to disciplinary action. Reports of unauthorized use of equipment may be made to the Internal Affairs Bureau.

HEALTH & SAFETY REPORTING

There are no known health and safety issues with thermographic 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 thermographic cameras mitigate the risk of impartial and biased law enforcement. Thermographic cameras only process the infrared light being omitted by any person or object into heat signature video. The NYPD does not record, store or retain any heat signature video or temperature data created by thermographic cameras. Thermographic cameras do not use facial recognition technologies. Other than the processing of the infrared light emitted by a person or object, the devices do not contain biometric measuring capabilities.

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.