DIGITAL CAMERAS: IMPACT & USE POLICY

ABSTRACT

The New York City Police Department (NYPD) uses digital cameras to create still-images in order to enhance the quality of NYPD investigations, operations, and programs.

The NYPD produced this impact and use policy because digital cameras are capable of creating images of people, locations, license plates, and any other visual information within the range of the device, and sharing the images with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Digital cameras are used to create digital still-images, e.g. photographs, by focusing a single image onto digital light-sensors. The camera captures that image and digitally saves the image for later review and reproduction. Digital cameras provide an objective record of what occurs within the focal range of the camera.

The camera is housed so its appearance is not hidden or disguised in anyway. Digital cameras used by the NYPD are not part of a larger network of cameras. Digital cameras do not use artificial intelligence, machine learning, facial recognition, or any other biometric measurement technologies.

A digital camera application is imbedded into many NYPD issued personal electronic devices (PEDs).

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD digital camera policy seeks to balance the public safety benefits of this technology with individual privacy. The NYPD must use digital cameras 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.

Digital cameras are used daily as needed. Usually, digital cameras are utilized for documentation purposes, such as memorializing: crime scenes and evidence, the location of physical evidence found at crime scenes, victim injuries, property damage, line-up identification procedures, personnel identification, trainings, NYPD attended community events, arrest photographs, etc. NYPD personnel may only use digital cameras to execute their lawful duties, which relate only to official business of the NYPD.

Court authorization is not necessary to use digital cameras to collect images of a location where there is no reasonable expectation of privacy, or if exigent circumstances exist. However, a warrant must first be obtained before the NYPD can use digital cameras to collect images where there is a reasonable expectation of privacy when there is no indication of exigent circumstances.

1 For additional information on PEDs, please refer to the PED impact and use statement.

DRAFT FOR PUBLIC COMMENT: POSTED JANUARY 11, 2021
The warrant is obtained with the aid of the prosecutor with proper jurisdiction. The warrant must contain a finding of probable cause by a judge, as well as an explicit authorization for entry into the queried location.

If exigent circumstances exist, an NYPD investigator must have probable cause to believe (1) a crime designated under Criminal Procedure Law Section 700.05(8), Penal Law Sections 460.10(1), 215.57, 215.56, or 240.30 has been committed, is in progress or is about to be committed; (2) an emergency exists as result of the criminal conduct; (3) there is an immediate urgent need for assistance due to an imminent danger of serious bodily injury or death to any person; and (4) the effort to locate a suspect is being undertaken with the primary concern of preventing serious injury or death and is not primarily motivated by an intent to arrest and seize evidence. The possibility of flight of a suspect does not on its own constitute exigent circumstances.

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 digital cameras.

Any NYPD investigation involving political activity is conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity in accordance with the Revised Handschu Guidelines.

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

**SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

Digital cameras are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a squad supervisor must periodically inspect and account for the digital cameras.

Images are retained within an appropriate NYPD computer or case management system. Only authorized users have access to the images. 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.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. All NYPD computer systems are managed by a user permission hierarchy based on rank.
DIGITAL CAMERAS: 
IMPACT & USE POLICY

and role via Active Directory authentication. The active directory 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 is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with 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 any system will subject employees to administrative and potentially criminal penalties.

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

Data recorded by NYPD digital cameras are stored locally, either on the device itself or within a memory card inserted into the device. Once the memory of the digital camera reaches maximum capacity, the digital camera cannot create new images until the memory is cleared.

Images relevant to an investigation are stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing case management and computer 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.

Images stored within NYPD computer and case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Images may only be used for legitimate law enforcement purposes or official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings.

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

DRAFT FOR PUBLIC COMMENT: 
POSTED JANUARY 11, 2021
DIGITAL CAMERAS: IMPACT & USE POLICY

POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request images created by the use of NYPD digital 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 digital camera obtains images related to a criminal case, the NYPD will turn the images over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the images to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request images 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 images or information related to it to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, the images or related 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.
DIGITAL CAMERAS:
IMPACT & USE POLICY

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 digital 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 digital camera 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.

TRAINING

NYPD personnel using digital cameras receive command level training on the proper operation of the technology. NYPD personnel must use all digital cameras in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

All members of the NYPD are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system 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).
Digitals Cameras: Impact & Use Policy

Supervisors of personnel utilizing digital cameras are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all images 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 associated with digital 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 digital cameras mitigate the risk of impartial and biased law enforcement. Digital cameras only memorialize what occurs within the focal range of the camera as a still photograph. Digital cameras do not use artificial intelligence, machine learning, facial recognition, or any other 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.