DRONE DETECTION SYSTEMS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that drone detection systems 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 drone detection systems rules of use.	Added language clarifying drone detection systems rules of use.
Expanded upon drone detection systems safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to drone detection systems when job duties no longer require access.
Expanded upon drone detection systems data retention.	Added language to reflect NYPD obligations under federal, state and local record retention laws.
Expanded upon drone detection systems external entities section.	Added language to reflect the NYPD obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

The growing popularity of consumer unmanned aircraft systems (UAS), commonly referred to as "drones," poses potential safety and security challenges at large-scale gatherings and events in New York City. Traditional security and observation methods may not adequately detect unlawful operations of UAS, leaving these sites vulnerable to consequential incidents.

The New York City Police Department (NYPD) uses drone detection systems to detect, identify, and monitor UAS flying within New York City airspace posing a credible threat to public safety, city facilities, and critical infrastructure. Drone detection systems are used at large-scale events in New York City, including: parades, sporting events, street celebrations (Times Square on New Year's Eve), and other large gatherings. The technology is commonly used in cooperation with other federal law enforcement agencies who are also charged with monitoring such events.

The NYPD produced this impact and use policy because drone detection systems have the ability to process audio signals, geo-location data, and video and still photographs of UAS in-flight or subject to tracking.

CAPABILITIES OF THE TECHNOLOGY

NYPD drone detection systems are a comprehensive platform capable of identifying UAS communication links. Through the use of omni-directional, directional, and high-gain directional antennas and radio-frequency sensors, drone detection systems can detect UAS in flight within a set range, locate the UAS and the general location of its operator, identify the speed and altitude of the UAS and track the UAS flight path. The detection radius of the technology can span several miles depending on configuration.

NYPD drone detection systems can also implement geo-fence zones around fixed locations within the City. Geo-fencing allows the creation of warning zones and alert zones surrounding the airspace above a fixed location.

The drone detection systems operated by the NYPD detect, identify, and track UAS that may present a threat to public safety. The technology does not mitigate or interdict UAS flight. Further, NYPD drone detection systems do not use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD's drone detection systems policy seeks to balance the public safety benefits of this technology with individual privacy. The NYPD must use drone detection systems 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 drone detection systems are only used by trained NYPD personnel assigned to the Counterterrorism Division (CTD) and my only be used for legitimate law enforcement purposes.

Drone detection systems implicate a variety of federal and state laws relating to surveillance and the capturing of electronic communications. The use of this technology is guided by reviews conducted by the NYPD Legal Bureau to ensure that such usage is in compliance with state laws

related to eavesdropping as well as federal laws such as the Pen/Trap and Trace Device Statute (18 U.S.C. §§ 3121-3127) and the Wiretapping Act (18 U.S.C. §§ 2510 *et. seq*). Additionally, the NYPD is guided by advisories on drone detection systems provided by the Department of Justice, Department of Homeland Security, and the Federal Aviation Administration.

If such uses are not exempt under the aforementioned statutes, or if no exceptions to the warrant requirement exist, pen register or trap and trace orders can be obtained with assistance from the relevant prosecutor offices.

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 drone detection systems.

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 drone detection systems will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

When not in use, drone detection system equipment is securely stored in NYPD facilities, in a location that is inaccessible to the public. Drone detection system equipment is only accessible to NYPD personnel authorized to use the technology. A supervisor must periodically inspect and account for the devices.

Authorized users of drone detection systems are critically limited to NYPD CTD officers who have received training in the use of the technology. NYPD drone detection system access is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to the technologies 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).

Data associated with NYPD use of drone detection systems is retained on a secured third party cloud-based storage system and is encrypted both at rest and in transit. The data is transmitted over a secured stand-alone network. NYPD access to the cloud-based storage system is critically limited to NYPD personnel with on a need-to-know basis. Authorized users must be authenticated by a username and password. The cloud-based storage system can only be accessed by CTD officers using laptops that operate on a closed, secured network. Supervisors in the CTD also determine what additional security features need to be added to this technology.

The data collected through the NYPD's use of drone detection systems may be downloaded from the cloud-based storage system and stored within an appropriate 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. Case management system access levels are 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)

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 employees to administrative and potentially criminal penalties.

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

Data associated with the NYPD's use of drone detection systems is stored on a secured third party cloud-based storage system for thirty (30) days before it is permanently deleted from the system. Only authorized users within CTD have access to the cloud-based storage system. Only those authorized CTD users can download drone detection system data for long-term retention. Data relevant to an investigation is stored in an appropriate NYPD computer or case management system.

Data associated with NYPD drone detection systems 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 NYPD drone detection system data is stored in 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.[1] 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.[2]

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).

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

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 retained 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 data obtained through the NYPD use of drone detection 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 Department policy.

EXTERNAL ENTITIES

If data obtained through the NYPD's use of drone detection technologies is related to a criminal case, the NYPD will turn it 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 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 the 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 related to this technology 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.

Drone detection technology does not record or retrieve personal identifying information. However, pursuant to NYPD policy and local law, members of the NYPD 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 drone detection 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 drone detection 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 data associated with NYPD drone detection systems 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 CTD personnel using drone detection technology are trained by the NYPD vendor for drone detection technology on its proper operation, including the use of any supporting tools.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors in CTD are responsible for the security and proper utilization of drone detection systems 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.

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).

NYPD Policy requires authorized users to maintain the confidentiality of accessible information and forbids improper dissemination of information, access beyond authorization granted by the NYPD, and breach of confidentiality.

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

As a general matter, as this technology continues to evolve, there have been studies conducted on detection challenges, particularly the ability of the technology to potentially interfere with other lawful aircraft communication systems.[3] Nonetheless, there are no known health and safety issues associated with the drone detection systems operated by the NYPD or its associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD drone detection systems mitigate the risk of impartial and biased law enforcement. NYPD drone detection technologies detect UAS within a given range, locate the UAS and its operator, identify the speed and altitude of the aircraft, as well as track and plot the UAV flight path. The detection radius of

[3] *See generally* Arthur Michael Holland, *Counter-Drone Systems: 2nd Edition*, CTR. FOR THE STUDY OF THE DRONE 7-13 (DEC. 2019), https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf.

the technology can span several miles depending on configuration. Drone detection systems 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.