GLOBAL POSITIONING SYSTEM TRACKING DEVICES:
IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that GPS tracking devices do not use artificial intelligence or machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon GPS tracking device rules of use.	Added language clarifying GPS tracking device rules of use. Added language to reflect that GPS tracking devices may only be used for legitimate law enforcement purposes.
Expanded upon court authorization language for GPS tracking devices.	Added language clarifying what needs to be demonstrated during an application for court authorization.
Expanded upon GPS tracking device safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to GPS tracking devices when job duties no longer require access.
Expanded upon GPS tracking device data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon GPS tracking device external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

The New York City Police Department (NYPD) uses global positioning system (GPS) tracking devices to provide NYPD personnel with real-time location data related to a subject of criminal investigation.

The use of GPS tracking devices allows NYPD personnel to obtain location data in situations where it is impractical or impossible to manually obtain that data through physical surveillance of a subject by NYPD personnel. Manual physical surveillance is resource intensive and inherently carries a risk that a subject may observe surveilling NYPD personnel and jeopardize the underlying investigation.

The NYPD produced this impact and use policy because its GPS tracking devices collect, retain, process, and share location data for subjects of criminal investigations.

CAPABILITIES OF THE TECHNOLOGY

GPS tracking devices are capable of identifying or estimating the geographic position of the tracking device. The device is placed on a movable, physical object related to a subject of criminal investigation

GPS tracking devices operate by receiving and processing radio signals that are continuously transmitted by global positioning satellites circling Earth's orbit, which generate a set of coordinates (i.e., latitude and longitude) used to determine the location of the device and, accordingly, location data relevant to a criminal investigation.

NYPD GPS tracking devices may be used to track the location of the device in real-time. Location data may also be downloaded from the tracking device itself for later review. Hardware and software connected to the use of GPS tracking devices support NYPD personnel in downloading, reviewing, and using the obtained location data.

GPS tracking devices only provide NYPD personnel with a set of location coordinates (i.e., latitude and longitude) of the device. GPS tracking devices are not capable of collecting any other data in the vicinity of the device. GPS tracking devices do use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD GPS tracking device policy seeks to balance the public safety benefits of this technology with individual privacy. GPS tracking devices 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.

Supervisory personnel must be consulted prior to use of GPS tracking devices. The underlying facts are considered on a case-by-case basis prior to the utilization of the technology. NYPD GPS tracking devices may only be used for legitimate law enforcement purposes.

In most cases, NYPD investigators must first obtain a search warrant allowing for the use of GPS tracking devices. The warrant is obtained with the aid of the prosecutor with proper jurisdiction. The NYPD investigator and prosecutor must make an application to a judge for a search warrant.

The search warrant can only be issued by a judge. The application must be made under oath. For a judge to grant a search warrant, the judge must find there is probable cause to believe a person has committed, is committing, or is about to commit a crime,[1] and the use of a GPS tracking device will be relevant to the investigation. NYPD personnel must use the GPS tracking device in accordance with the terms of the warrant.

GPS tracking devices may also be used without court authorization on NYPD property or with individual consent.

All necessary documentation, including a copy of search warrant under the requisite circumstances, must be provided to NYPD personnel who will install the GPS tracking device. No GPS tracking devices will be installed without all required documentation described in this impact and use policy.

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 GPS tracking devices.

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.

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 GPS tracking devices will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

GPS tracking devices are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the devices.

Software connected to the use of GPS tracking devices is part of a closed network, used solely in connection with operating the devices. Only specific NYPD personnel can install a GPS tracking device and grant NYPD personnel access to the supporting hardware and software. Authorized users of the cell-site simulator software are authenticated by a username and password. GPS tracking device software can only be accessed on a closed, stand-alone network. Data at rest and in transit is encrypted to military standards.

[1] A crime is: 1) any crime as defined by N.Y. Crim. Proc. Law § 700.05(8); 2) any criminal act as defined by N.Y. Penal Law § 460.10(1); 3) Bail Jumping in the First and Second Degree as defined by N.Y. Penal Law §§ 215.57 and 215.56; or 4) Aggravated Harassment in the Second Degree as defined by N.Y. Penal Law § 240.30. If the NYPD is assisting with a federal investigation, an application for a search warrant can be made in federal court if the information likely to be obtained is relevant to an ongoing federal criminal investigation.

Location data is retained within an NYPD computer or case management system. Only authorized users have access to this data. 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 data accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose data 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 data. 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 data from the NYPD and determine that the release of data 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

GPS tracking devices retain location data locally on the device itself, as well as transmit real-time location to a remote server that is accessible through associated software. Access to the associated software is granted for the time period authorized by the court order obtained by the NYPD investigator. After location data is downloaded and provided to the assigned NYPD investigator, the location data is deleted from the GPS tracking device and connected hardware and software.

GPS tracking device location data 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. Location data relevant to an investigation 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.

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. 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.

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 location 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 location data obtained from NYPD use of GPS tracking devices 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 GPS tracking device obtains data relevant to a criminal case, the NYPD will turn the data over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the material 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 to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Data is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, data 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 data obtained from the NYPD, limiting disclosure of that data without NYPD approval, and notifying the NYPD when the external entity receives a request for that data 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 GPS tracking devices 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 GPS tracking devices 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 NYPD GPS tracking devices 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 GPS tracking devices receive command level training on the proper operation of the technology and the associated equipment. NYPD personnel must use GPS tracking devices in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of a GPS tracking device, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing GPS tracking devices 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 with NYPD guidelines.

All 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).

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

There are no known health and safety issues associated with GPS tracking devices or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for GPS tracking devices mitigate the risk of impartial and biased law enforcement. NYPD GPS tracking devices may be used to track the location of a GPS compatible device. The technology is only used after a NYPD investigator obtains court authorization for its use. GPS tracking devices 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. 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.