



**GLOBAL POSITIONING SYSTEM  
TRACKING DEVICES:  
IMPACT AND USE POLICY**

**UPDATED: FEBRUARY 4, 2026**

**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.

**GLOBAL POSITIONING SYSTEM (GPS) TRACKING DEVICES ADDENDUM**

<b>Date of Addendum</b>	<b>Description of Addendum</b>
April 11, 2023	GPS tracking devices used to track fleeing vehicles in limited circumstances will be tested by the NYPD for a 90-day period.
September 13, 2024	Included additional details regarding the rules, processes, guidelines, and health and safety concerns associated with the use of GPS Tracking technology.  Updated data retention practices to reflect current policy.

**GLOBAL POSITIONING SYSTEM (GPS) TRACKING DEVICES REVISION**

<b>Date of Revision</b>	<b>Description of Revision</b>
February 4, 2026	This IUP was revised to comply with the recently passed amendment to the POST Act, Local Law 56 of 2025.

## **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 a 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. 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. These 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.

The GPS tracking devices used by the NYPD are manufactured by MetOcean. The devices may be manually attached to movable, physical items pertaining to the subject of a criminal investigation that NYPD personnel want to track. GPS tracking devices may be used to track the location of the object in real-time. Hardware and software connected to the use of GPS tracking devices support NYPD personnel in downloading, reviewing, and using the obtained location data. The battery life of traditional GPS tracking devices varies, but ranges from approximately 14 to 30 days.

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

## **RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY**

---

NYPD's 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.

GPS tracking devices may only be used for legitimate law enforcement purposes. 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.

***Court Authorization:*** In most circumstances, NYPD investigators must first obtain a warrant allowing for the use of GPS tracking devices. Warrants are obtained with the aid of the prosecutor with proper jurisdiction. The NYPD investigator and prosecutor must make an application, under oath, to a judge for a warrant. For a judge to grant a warrant, the judge must find there is probable cause, 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. All necessary documentation, including a copy of the warrant under the requisite circumstances, must be provided to NYPD personnel who will install the GPS tracking device.

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

***Additional Guidelines:*** If necessary, the Intelligence Division will determine the need for GPS tracking devices for NYPD investigations involving political activity. The Intelligence Division is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Revised *Handschu* Guidelines.

As with all NYPD operations, no person will be the subject of police action 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.

***Addendum Obligations:*** 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.

### **SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

***Physical Safeguards & Security Measures:*** All 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. Access to GPS tracking devices is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to the devices is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

***Data Safeguards & Security Measures:*** 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 tracking software are authenticated by a username and password. GPS tracking device software can only be accessed on a closed, stand-alone network.

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 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 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 from 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. The location data for these devices will be retained for a period of 3 years unless data has been identified to be retained for security purposes or for criminal investigations.

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 litigation, 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 NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. The retention period of a “case investigation record” depends on its classification and 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 they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought.

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 data collected by the NYPD through its 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 the law.

### **EXTERNAL ENTITIES**

Entities outside of the NYPD do not have direct access to the information and data collected by NYPD’s GPS tracking devices.

If a GPS tracking device obtains location data relevant to a criminal case, the NYPD will turn the data over to the prosecutor with jurisdiction over the matter in accordance with criminal discovery laws. Prosecutors will provide the material to the defendant(s) in accordance with the same criminal discovery laws.

Other law enforcement agencies may request location 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. Location 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, GPS tracking device location 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.

***Vendors & Contractors:*** The NYPD purchases GPS tracking devices and associated equipment or 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 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 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 within 24 hours. The NYPD must make reasonable efforts to notify individuals affected 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 publicly 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 GPS tracking devices, including the reasons for its use, must be discussed with a supervisor. Officers utilizing any GPS tracking devices are directed to inspect the equipment prior to use and notify their supervisors immediately if the equipment is damaged or becomes inoperable at any point. Supervisors 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 tests or reports regarding the health and safety effects of GPS tracking devices. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of GPS tracking devices.

### **DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY**

The NYPD has implemented significant safeguards to ensure that GPS tracking devices are used effectively and responsibly. The NYPD does not believe that this technology is being used in a manner that disparately impacts any protected groups as defined in the New York City Human Rights Law.

The safeguards and audit protocols built into this impact and use policy for GPS tracking devices help to mitigate the risk of partial and biased law enforcement. The NYPD uses GPS tracking devices to enhance public safety and assist in investigations. In most cases, GPS tracking devices are only used after a NYPD investigator obtains court authorization for its use. Access is restricted

to authorized personnel. GPS tracking devices do not use any biometric measurement technologies. Based on these safeguards, any theoretical risks of GPS tracking devices disparately impacting protected groups are effectively mitigated.

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.