PROJECTILE GLOBAL POSITIONING SYSTEM TRACKING DEVICES: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

PROJECTILE GLOBAL POSITIONING SYSTEM (GPS) TRACKING DEVICES REVISION

Date of Revision	Description of Revision
February 4, 2026	This impact and use policy was drafted to comply with the recently passed amendment to the POST Act, Local Law 56 of 2025. This impact and use policy was de-grouped from the GPS Tracking Devices impact and use policy,[1] given the differing functionality of projectile GPS tracking devices.

[1] For additional information, please refer to the GPS Tracking Devices impact and use policy.

ABSTRACT

The New York City Police Department utilizes projectile global positioning systems (GPS) tracking devices, known as StarChase, in an effort to reduce the frequency of vehicle pursuits.

StarChase provides a means to remotely track vehicles by attaching a projectile GPS enabled device through either a vehicle-mounted or handheld device. By remotely attaching StarChase onto a fleeing vehicle in limited circumstances, NYPD personnel can locate and track vehicles without engaging in vehicle pursuits.

The NYPD produced this impact and use policy because StarChase collects, retains, processes, and shares location data for subjects of criminal investigations.

CAPABILITIES OF THE TECHNOLOGY

StarChase is manufactured by Starchase LLC. It operates 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 device's location.

StarChase allows officers to attach a projectile GPS tracking device to a moving vehicle through a vehicle mounted GPS launcher unit (StarChase Guardian VX System) or a handheld GPS launcher unit (StarChase Guardian HX System). The vehicle-mounted StarChase allows officers to launch a projectile GPS tracking device via a compressed-air launcher from the front of a patrol vehicle. The hand-held device serves as a portable alternative to the vehicle-mounted version. It uses a single shot, air-powered launcher to deploy a projectile GPS tracking device. The battery life of StarChase is approximately 8 to 10 hours.

Once attached to the suspect vehicle, the device broadcasts real-time position mapping data that NYPD personnel then use to locate the suspect vehicle on a secure web-based platform. Location data may be downloaded for later review through the connected software.

While StarChase is used to mitigate the need for high-speed pursuits, its use is limited by NYPD policy, as discussed in more detail in the 'Rules, Processes & Guidelines Relating to Use of the Technology' section. StarChase only provides NYPD personnel with a set of location coordinates (i.e., latitude and longitude) and is not capable of collecting any other data in its vicinity. StarChase does not use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD's projectile 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.

Court Authorization: StarChase may only be used for legitimate law enforcement purposes. In limited, exigent circumstances, StarChase may be used to remotely attach to vehicles without first obtaining a warrant. These limited circumstances include when there is probable cause to believe that the vehicle, or occupant of the vehicle, is connected to, or has committed, one or more of the following crimes: (1) any crime that resulted in death (e.g., homicide, leaving the scene of an fatal accident, etc.), (2) robbery, (3) burglary, (4) felony assault, (5) criminal possession of a firearm,

(6) felony criminal possession of a weapon, (7) reckless endangerment, or (8) reckless driving where the driver is being used as a means to cause serious physical injury or death to a uniformed member of the service or other person present. StarChase may also be used if a uniformed member can clearly articulate their particularized basis for believing that the subject vehicle is stolen.

While StarChase may initially be deployed without a warrant, these circumstances do not allow for the indefinite tracking of a vehicle. If uniformed members of the service are unable to locate the StarChase-tagged vehicle after a reasonable amount of time after deploying StarChase, officers must obtain a warrant to continue tracking the vehicle's location through GPS.

When necessary, warrants are obtained with the aid of the prosecutor with proper jurisdiction. NYPD personnel and the prosecutor must make an application to a judge for a warrant. The application must be made under oath. 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.

StarChase may only be used by NYPD personnel that have been trained in its operation. NYPD personnel must comply with all aspects of the NYPD's vehicle pursuit policy. NYPD personnel must stop pursuing the target vehicle once it is confirmed that StarChase successfully attached to a vehicle. StarChase may only be used to track a vehicle from the time it flees until the vehicle and/or passengers can be safely recovered or apprehended.

StarChase cannot be deployed on any vehicle designed to be operated with fewer than four wheels, or any vehicle that does not have a completely enclosed passenger compartment (e.g., motorcycle, ATV, convertibles with top down, etc.). NYPD personnel are prohibited from engaging in a vehicle pursuit solely for the purpose of using StarChase and cannot use the device in unsafe conditions. Handheld models of StarChase may only be operated and deployed by the passenger officer.

Additional Guidelines: If necessary, the Intelligence Division will determine the need for the use of StarChase 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 StarChase 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 StarChase.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

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

Data Safeguards & Security Measures: StarChase data is stored in a secure cloud environment. Data at rest and in transit is encrypted to military standards. StarChase software is part of a closed, stand-alone network, used solely in connection with operating the devices. Only specific NYPD personnel can access the supporting hardware and software. Authorized users of StarChase are authenticated by a username and password.

Location data is downloaded and 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

StarChase retains location data locally on the device itself, as well as transmits real-time location data to a remote server that is accessible through associated software. Access to the associated software is granted for the time period the device is in use. 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.

StarChase location data may only be used for legitimate law enforcement purposes. 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 StarChase 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

Currently, the NYPD has a data sharing agreement with the Westchester County Department of Public Safety with respect to StarChase. The agreement includes the sharing of location data, allowing both the NYPD to track vehicles when StarChase projectiles are attached by Westchester, and vice versa, streamlining assistance when pursuits cross respective jurisdictions. This agreement may be terminated at any time.

If StarChase 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, StarChase 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 StarChase 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 StarChase's 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 StarChase 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 StarChase receive command-level training on the proper operation of the technology and the associated equipment. NYPD personnel must use StarChase in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Only NYPD personnel specifically trained in StarChase's use may deploy it. Officers utilizing StarChase are directed to inspect it 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

StarChase is designed for safe and effective remote adhesion of a GPS tracking device when used in compliance with the criteria explained in the 'Rules, Processes & Guidelines Relating to Use of the Technology' section of this impact and use policy. To ensure safety, the manufacturer advises

operators to only aim the device at vehicles and never at individuals. While there do not appear to be any safety incidents reported, misuse of StarChase may result in unintended injury or death. The NYPD addresses possible injury during StarChase deployment by instructing officers to comply with NYPD procedures for vehicle deployment and reporting of injuries.

DISPARATE IMPACTS OF THE TECHNOLOGY

The NYPD has implemented significant restrictions and safeguards to ensure that StarChase is 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 StarChase help mitigate the risk of partial and biased law enforcement. The NYPD uses StarChase to enhance public safety, assist in investigations, and reduce high-speed pursuits. Access is restricted to authorized personnel. While StarChase may be used to remotely attach to fleeing vehicles, this tracking is not indefinite. Officers are directed to obtain a warrant to continue tracking if they are unable to locate the vehicle after a reasonable amount of time. StarChase does not use any biometric measurement technologies. Based on these safeguards, any theoretical risks of StarChase 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.