WiFi GEOLOCATION TRACKING DEVICES: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that WiFi geolocation 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 abstract for WiFi geolocation tracking device.	Added language clarifying that as of final policy publication, WiFi geolocation tracking devices have not been used by the NYPD beyond the testing of the devices.
Expanded upon WiFi geolocation tracking device rules of use.	Added language clarifying GPS tracking device rules of use.
Expanded upon court authorization language for WiFi geolocation tracking device.	Expanded on exigent circumstances language.
Expanded upon WiFi geolocation tracking device safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to WiFi geolocation tracking devices when job duties no longer require access.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

As of April 11, 2020, the NYPD has never used WiFi geolocation tracking devices outside of testing the devices. However, WiFi geolocation tracking devices can aid NYPD personnel in locating criminal suspects and finding missing persons and victims of abductions.

The NYPD produced this impact and use policy because WiFi geolocation tracking devices can process location information of WiFi enabled devices and share the data with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

WiFi geolocation tracking devices can identify or estimate the geographic position of WiFi connected devices in real-time. In response to signals emitted by the WiFi geolocation tracking device, WiFi enabled devices within the proximity of the WiFi geolocation tracking device identify it as a potential WiFi network. WiFi enabled devices in the area then transmit signals to the WiFi geolocation tracking device, which identify the WiFi enabled device in the same way it would with a traditional WiFi network.

By functioning as a potential WiFi network, WiFi geolocation tracking devices process limited information from mobile devices. WiFi geolocation tracking devices provide only the relative signal strength and general direction of the subject mobile device; the devices do not function as a global positioning locator.

NYPD WiFi geolocation tracking devices do not record, store, or retain any of the processed location data. NYPD WiFi geolocation tracking devices do not collect the contents of any communication or any data contained on electronic devices, including emails, text messages, contact lists, or images. WiFi geolocation tracking devices cannot be used to engage in unauthorized access or "hacking" of electronic devices.

WiFi geolocation tracking devices do not use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD WiFi geolocation tracking device policy seeks to balance the public safety benefits of this technology with individual privacy. WiFi geolocation 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 WiFi geolocation tracking devices. The underlying facts will be considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purpose to utilize the technology in a given circumstance.

WiFi geolocation tracking devices can only be used under exigent circumstances, therefore the NYPD would not seek court authorization prior to using the device.

In order to use WiFi geolocation tracking devices, 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.

When exigent circumstances exist, the NYPD investigator must first document the nature of the emergency before WiFi geolocation tracking devices may be used and contact the local prosecutorial agency to obtain a search warrant. While the WiFi geolocation tracking device may be used prior to issuance of the court order, the order must be obtained within forty-eight (48) hours following its use. A search warrant is not required when a WiFi geolocation tracking device is used to assist NYPD personnel in searching for a missing or suicidal person.

WiFi geolocation tracking devices may only be used by NYPD personnel for legitimate law enforcement purposes, and access to WiFi geolocation tracking devices is critically limited. Only members of the NYPD Technical Assistance Response Unit (TARU) can access and operate the WiFi geolocation tracking devices and associated equipment. WiFi geolocation tracking devices will only be used after TARU has received all proper documentation including: the complaint number and TARU Exigent Circumstances Declaration or emergency warrant. NYPD personnel involved in the use of WiFi geolocation tracking devices may only utilize the technology to execute their lawful duties, which relate only to official business of the NYPD.

WiFi geolocation devices will only be used while the exigency or emergency persists. Upon expiration of such circumstances, use of the WiFi geolocation devices will be terminated, and the physical device will be returned its command.

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 use of WiFi geolocation 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 WiFi geolocation tracking devices will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

WiFi geolocation tracking devices are securely stored in NYPD facilities in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the devices. Access to WiFi geolocation tracking devices is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to WiFi geolocation tracking device technology is removed when access 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).

Authorized users of WiFi geolocation tracking devices are authenticated by a username and password. NYPD WiFi geolocation tracking devices operate on a closed, stand-alone network. The network can only be accessed by limited TARU laptops. A physical, wired connection between the WiFi geolocation tracking device and the laptop is required for the device to function.

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 all computer 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

WiFi geolocation tracking devices will only be used while the exigency or emergency persists. Upon expiration of the exigency, use of the WiFi geolocation tracking device will be terminated, and the physical device returned its command.

As the NYPD cannot record, store, or retain any information processed through WiFi geolocation tracking devices, there are no policies or procedures relating to retention, access, and use of collected data.

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

Members of the public may request information related to NYPD use of WiFi geolocation 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

WiFi geolocation tracking devices are operated exclusively by NYPD personnel, and no entities outside the NYPD have access to the devices. As the NYPD cannot record, store, or retain any information processed by WiFi geolocation tracking devices, there is no data that can be provided to external entities.

TRAINING

NYPD personnel from the Technical Assistance and Response Unit (TARU) can operate WiFi geolocation tracking devices and are trained in the proper operation of the technology and the associated equipment. WiFi geolocation tracking devices must be used in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of WiFi geolocation tracking devices, including the reasons for its use, must be discussed with a supervisor. Only TARU personnel can operate WiFi geolocation tracking devices and associated software, which may only be done after receiving proper documentation, including the TARU Exigent Circumstances Declaration.

Supervisors of personnel utilizing WiFi geolocation tracking devices are responsible for security and proper utilization of the technology and associated equipment. Supervisors must periodically inspect and account for the devices.

All NYPD personnel are advised that NYPD equipment is intended for the purposes of conducting official business. The misuse of any 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).

HEALTH & SAFETY REPORTING

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

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

While WiFi geolocation tracking devices have not been used outside of testing, the safeguards and audit protocols built into this impact and use policy for NYPD WiFi geolocation tracking devices mitigate the risk of impartial and biased law enforcement. The devices only process information connected to WiFi enabled devices within range and provide only the relative signal strength and general direction of a subject mobile device. WiFi geolocation tracking devices cannot retain any information obtained in the course of use, therefore the NYPD cannot record, store, or retain any information processed through WiFi geolocation tracking devices. WiFi geolocation 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.