ABSTRACT

WiFi geolocation tracking devices 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.

WiFi geolocation tracking devices used by the NYPD 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. The NYPD does not use its WiFi geolocation tracking devices to engage in unauthorized access or “hacking” of electronic devices. WiFi geolocation tracking devices do not use artificial intelligence, machine learning, or any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD’s 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.

The NYPD does not use its WiFi geolocation tracking devices to engage in unauthorized access or “hacking” of electronic devices.

The NYPD only uses its WiFi geolocation tracking devices under exigent circumstances. WiFi geolocation tracking devices may be deployed prior to obtaining a probable cause order. In those situations 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.

Even if exigent circumstances exist, the NYPD investigator must first document the nature of the emergency before the WiFi geolocation tracking device is used. Additionally, a court order must be obtained soon-thereafter by the NYPD investigator with the aid of a prosecutor with proper jurisdiction.

Supervisory personnel must be consulted prior to use of WiFi geolocation tracking devices. The underlying facts are 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.

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 the any additional uses 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.

**SAFEGUARDS & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

WiFi geolocation 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.

WiFi geolocation tracking devices do not retain any information obtained during its use, and the NYPD does not record, store, or retain any information processed through WiFi geolocation tracking devices.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.
POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS, & USE OF THE DATA

As the NYPD does not 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 does not 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) operate WiFi geolocation tracking devices and are trained in the proper operation of the technology and the associated equipment. NYPD personnel must use WiFi geolocation tracking devices 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. 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

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. WiFi geolocation tracking 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 do not retain any information obtained in the course of use, and the NYPD does not record, store, or retain any information processed through WiFi geolocation tracking devices. WiFi geolocation tracking devices do not use artificial intelligence, machine learning, or 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.