



CELL-SITE SIMULATORS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that cell-site simulators do not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon cell-site simulator rules of use.	Added language clarifying cell-site simulator rules of use.
Clarified court authorization for cell-site simulators.	‘Probable cause order’ and ‘court order’ was replaced with ‘search warrant.’
Expanded upon cell-site simulator safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to cell-site simulators when job duties no longer require access.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

Cell-site simulators¹ are used in the location or identification of mobile devices. The technology supports locating missing persons, victims of abductions, and criminal suspects. The New York City Police Department (NYPD) uses cell-site simulators in furtherance of these public safety responsibilities.

The NYPD produced this impact and use policy because cell-site simulators are capable of collecting and sharing cellular device location data with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Cell-site simulators function by behaving like a traditional networked cell tower. In response to signals emitted by a cell-site simulator, cellular devices within the proximity of the cell-site simulator identify it as the most attractive cell tower in the area. When the simulator is within the cellular device's signal range, it measures the device's signal strength and determines the location of the phone.

Every device capable of connecting to a cellular network through a cell tower is assigned an industry-standard unique-identifying number by the device's manufacturer or cellular network provider. Cell-site simulators are used either to locate a cellular device where the unique-identifying number is known or to identify a cellular device with an unknown unique-identifying number.

By functioning as a cell tower, cell-site simulators acquire limited information from cellular devices. Cell-site simulators provide only the relative signal strength and general direction of a cellular device; they do not function as a global positioning locator.

Cell-site simulators are not used to collect the contents of any communication or any data contained on the device itself. Cell-site simulators also do not capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an account holder's name, address, or telephone number).

Cell-site simulators are used in conjunction with vendor-provided software. The associated software displays the location data processed by the cell-site simulator in a format usable by NYPD personnel. Cell-site simulators used by the NYPD do not retain or record any of the data or information received by the cell-site simulator or associated software.

Cell-site simulators do not use any biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD cell-site simulator policy seeks to balance the public safety benefits of this technology with individual privacy. Cell-site simulators must be used in a manner consistent with the requirements

¹ Cell-site simulators are known colloquially as "Stingrays." Originally, the Stingray was a specific cell-site simulator manufactured by the Harris Corporation. The term Stingray has become a generic name to reference cell-site simulators generally.

and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

In most cases, NYPD investigators must first obtain a search warrant allowing for the use of the device. The search warrant is obtained with the aid of a 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,² and the use of a cell-site simulator will be relevant to the investigation. NYPD personnel must use the cell-site simulator in accordance with the terms of the warrant.

However, a cell-site simulator may be used prior to obtaining a search warrant if exigent circumstances exist. In those instances, 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 a cell-site simulator will be used and contact the local prosecutorial agency to obtain a search warrant. While the cell-site simulator may be used prior to issuance of the search warrant, the warrant must be obtained within forty-eight (48) hours following its use. A search warrant is not required when a cell-site simulator is used to assist NYPD personnel in searching for a missing or suicidal person.

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

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 cell-site simulators.

² 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.

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 cell-site simulators or associated software will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Cell-sites simulators are securely stored within NYPD facilities when not in use, in a location inaccessible to the public. Additionally, a supervisor must periodically inspect and account for all equipment. Access to cell-site simulators is limited to TARU personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD cell-site simulator 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 the cell-site simulator software are authenticated by a username and password. Access to the software is critically limited to TARU personnel who have received training in the use of the technology. Cell-site simulator software can only be accessed by TARU on laptops that operate on a closed, stand-alone network. The network utilizes industry best standard best practices and systems to prevent external penetration and unauthorized usage.

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

Cell-site simulators will only be used for the time period authorized by the search warrant obtained by the NYPD investigator, or while the exigency or emergency persists. Upon expiration of the court order or exigent circumstances, use of the cell-site simulator in connection to that particular investigation is terminated, and the physical device is returned its command.

As the NYPD cannot record, store, or retain any of the data processed cell-site simulators, 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 cell-site simulators pursuant to 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

No external entities have access to NYPD cell-site simulators or the associated software. Cell-site simulators do not record, store, or retain any of the signals or data processed by the device.

TRAINING

TARU personnel are trained in the use and operation of cell-site simulators and the associated software by the vendor providing the technology. NYPD personnel must use cell-site simulators and the associated software in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The NYPD investigator requesting the cell-site simulator must discuss the reasons for its deployment with their supervisor. Only TARU personnel can operate cell-site simulator and associated software, which may only be done after receiving proper documentation. A cell-site simulator will not be used without proper documentation, even in exigent circumstances.

Supervisors of personnel utilizing NYPD's cell-site simulator technologies are responsible for security and proper utilization of the technology and associated equipment.

All NYPD personnel are advised that NYPD equipment is intended for the purposes of conducting official business. The misuse of 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 with cell-site simulators or the associated software.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD cell-site simulators mitigate the risk of impartial and biased law enforcement. Cell-site simulators are only used after a judicial finding of probable cause, or in limited exigent circumstances. Cell-site simulators only collect information and location data that would be sent to a traditional networked cell tower. None of the information or data is retained by the NYPD following the use of the technology. Cell-site simulators 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.