CALEA COLLECTION SYSTEM: IMPACT AND USE POLICY

NOVEMBER 24, 2023

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that CALEA collection system does not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon CALEA collection system rules of use.	Added language clarifying CALEA collection system rules of use.
Clarified court authorization for CALEA collection system.	'Court authorization' was replaced with 'PRTT order' or 'eavesdropping warrant,' as appropriate.
Expanded upon court authorization language for CALEA collection system.	The CALEA collection system is capable of performing functions requiring different levels of judicial scrutiny. Language was added clarifying what needs to be demonstrated in the different applications for court authorization.
Expanded upon CALEA collection system safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to CALEA collection system when job duties no longer require access.
Expanded upon CALEA collection system data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon CALEA collection system external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

CALEA COLLECTION SYSTEM ADDENDUM

Date of Addendum	Addendum Description
November 24, 2023	Updated to reflect the current number of facilities where the NYPD can operate the CALEA collection system.

ABSTRACT

The Communication Assistance for Law Enforcement Act (CALEA) is a set of laws and guidelines enacted to assist law enforcement agencies in conducting lawful interceptions of telecommunications. The CALEA collection system used by the New York City Police Department (NYPD) covertly collects, monitors, and records a variety of telecommunications transmissions. NYPD investigators operating the CALEA collection system are highly trained, and access to the technology itself is critically restricted.

The NYPD produced this impact and use policy because the CALEA collection system is capable of processing and sharing acoustic data and similar information with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

The CALEA collection system is the modern replacement of several different physical devices previously used to conduct a variety of lawful telecommunications interceptions. With the assistance of telecommunications carriers, the CALEA collection system replaces pen registers and trap and trace (PRTT) and wiretapping devices.

Historically, pen registers and trap and trace devices were two different pieces of equipment. Pen registers recorded all outgoing telephone numbers, or telephone numbers the queried telephone number dialed. Trap and trace devices recorded all incoming telephone numbers, or telephone numbers that called the queried telephone number. In the modern era, the CALEA collection system performs these functions.

Additionally, the CALEA collection system replaces the physical devices historically needed to covertly monitor telephone conversations; what is commonly known as a wiretap. The CALEA collection system is also capable of recording internet protocol (IP) addresses that visit a queried web address, network traffic, and the contents of short message service (SMS) and multimedia messaging service (MMS) messages.

The CALEA collection system does not use facial recognition or any other biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD CALEA collection system policy seeks to balance the public safety benefits of this technology with individual privacy. The CALEA collection system must be used by the NYPD 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.

NYPD investigators are almost always required to obtain court authorization prior to the utilization of the CALEA collection system. A PRTT order is obtained to use the CALEA collection system to covertly collect incoming and outgoing telephone numbers to a queried phone number, or to collect IP addresses that visit a queried web address. An eavesdropping warrant is obtained to use the CALEA collection system to covertly monitor telephone calls, SMS, MMS, and network traffic. The CALEA collection system may only be used for legitimate law enforcement purposes.

When seeking to use the PRTT capabilities of the CALEA collection system, the NYPD investigator and prosecutor must make the application to the judge for a PRTT order. The application must be made under oath. For a judge to grant a PRTT order, the judge must find reasonable suspicion that a designated crime[1] has been, is being, or is about to be committed and information likely to be obtained by using the PRTT function of CALEA is or will be relevant to the investigation of the designated crime. A judge can authorize the use of a PRTT for up to sixty (60) days. The NYPD investigator and prosecutor can apply to the judge for an extension of the PRTT order, and the judge must make similar findings to the original application to extend the PRTT order.

The CALEA collection system PRTT function may be utilized without first obtaining a warrant if exigent circumstances exist. In order to use the CALEA collection system in exigent circumstances without first obtaining a PRTT order, an NYPD investigator must reasonably believe: (1) a crime[2] has been committed, is being committed, 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 making it impracticable to prepare a written application without such risk occurring; 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. An emergency order must be obtained from the court with relevant jurisdiction within forty-eight (48) hours of the emergency use of the PRTT function.

When seeking to use the eavesdropping, or wiretapping, capabilities of the CALEA collection system, the NYPD investigator and prosecutor must make the application to the judge for an eavesdropping warrant. The application must be made under oath. For a judge to grant an eavesdropping warrant, the judge must find: 1) there is probable cause to believe a person is committing, has committed, or is about to commit a designated offense[3]; 2) there is probable cause to believe particular communications concerning the offense will be obtained; and 3) normal investigative procedures have been tried and failed, are unlikely to succeed if tried, or too dangerous to employ. An eavesdropping warrant cannot allow the use of the CALEA collection system eavesdropping function for any period longer than necessary; a maximum of thirty (30) days. The NYPD investigator and prosecutor can apply to the judge for an extension of the eavesdropping warrant, and the judge must make similar findings to the original application to extend the eavesdropping warrant.

[1] In New York, there must be reasonable suspicion that a designated crime has been, is being, or is about to be committed. A designated 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. If the NYPD is assisting with a federal investigation, an application for a PRTT order can be made in federal court if the information likely to be obtained is relevant to an ongoing federal criminal investigation.
[2] Please see the definition above.
[3] As related to an eavesdropping warrant application, a New York designated offense is defined by N.Y. Crim. Proc. Law § 700.05(8). If the NYPD is assisting with a federal investigation, designated offenses are defined by 18 U.S.C.S. § 2516(1) and (2).

The CALEA collection system eavesdropping function may be utilized without first obtaining a warrant if exigent circumstances exist. In order to use the CALEA collection system in exigent circumstances without first obtaining an eavesdropping warrant, an NYPD investigator must have probable cause to believe: 1) a person is committing, has committed, or is about to commit a designated offense[4]; (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 making it impracticable to prepare a written application without such risk occurring; 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. An emergency warrant granted by a state court judge must be obtained within twenty-four (24) hours of the emergency use of the eavesdropping function. An emergency warrant granted by a federal court judge must be obtained within forty-eight (48) hours of the emergency use of the eavesdropping function. An emergency eavesdropping order cannot be extended.

Access to the CALEA collection system is critically limited. Only members of the NYPD Technical Assistance Response Unit (TARU) can allow authorized users access to the CALEA collection system. TARU must be provided with all proper documentation including: the complaint number, queried phone number, and PRTT order or eavesdropping warrant in non-exigent circumstances, or TARU Exigent Circumstances Declaration and emergency PRTT order or eavesdropping warrant in exigent circumstances. These documents are shared with a telecommunication carrier. The telecommunication carrier will then provide access to the responsive information via the NYPD CALEA collection system pursuant to the terms of the court authorization or nature of the exigency. Only members of TARU can provide authorized users with access to the CALEA collection system.

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 use of the CALEA collection system.

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 the CALEA collection system will subject employees to administrative and potentially criminal penalties.

[4] Please see the definition above.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

The CALEA collection system resides on a closed, stand-alone network used solely in the operation of the system. The network utilizes industry standard best practices and systems to prevent unauthorized access.

The CALEA collection system can only be operated at five (5) NYPD facilities. Access to the facilities where the CALEA collection system can be used is limited to those authorized to be present by the PRTT order or eavesdropping warrant. Physical security protections include: guards, access logs, and locked facilities requiring badges or access cards for entry. The CALEA collection system cannot be accessed on general use NYPD desktops, NYPD issued portable electronic devices, or personal electronic devices.

Only TARU personnel can grant access to the CALEA collection system. Once access is granted, the investigator is authenticated through a unique username and password. Access is provided to the CALEA collection system after submitting all proper documentation to TARU. Access to the CALEA collection system lasts for as long as the court authorization allows, or as long as the exigent or emergency circumstances persist. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role. All digital records have a digital signature to ensure the records have not been tampered with.

CALEA collection system access control capabilities are limited to TARU personnel. CALEA collection system access control is removed when the technology is no longer necessary for TARU personnel to fulfill their duties (e.g., when TARU personnel are transferred to a different command).

Data obtained by the CALEA collection system is provided to NYPD personnel for long-term retention, including in computer or case management systems as appropriate. 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 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 NYPD computer and case management systems, 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

Upon conclusion of the investigation, exigency, or upon expiration of the court authorization, access to the CALEA collection system is terminated and data obtained during the investigation is provided to the NYPD investigator. Data is permanently deleted from the CALEA collection system on a first-in-first-out basis; when newly recorded data needs to be stored, it automatically records over the oldest data stored within the CALEA collection system. The data retention period within the CALEA collection system is dependent on storage capacity limitations.

Data collected by the CALEA collection system may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Relevant data is stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing case management and computer 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.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[5] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[6]

[5] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[6] *See* NYC Charter 3003.

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records 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 it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of, relevant case investigation record.

The misuse of any information 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 information obtained from NYPD use of the CALEA collection system 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

Personnel from other law enforcement agencies that have authorization to work in conjunction with the NYPD may have access to the CALEA collection system. Access is considered on a case by case basis.

If the CALEA collection system obtains material related to a criminal case, the NYPD will turn it over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the material to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request materials 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 information to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

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; or
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.

Government agencies at the local, state, and federal level, including law enforcement agencies other than the NYPD, have limited access to NYPD computer and case management systems. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases its CALEA collection system and associated equipment or Software as a Service (SaaS)/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 NYPD CALEA collection system 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 the CALEA collection system 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 as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected 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 publically available online.

TRAINING

Investigators operating the CALEA collection system receive specialized command level training and instruction in the technical use of the equipment. CALEA collection system manuals are readily available to all authorized users. Officers must operate the CALEA collection system in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of the CALEA collection system, including the reasons for its use, must be discussed with a supervisor. Only TARU may grant access to the NYPD CALEA collection system. Additionally, all proper documentation, including copies of court orders, must be provided to TARU. CALEA collection system access will not be provided if all proper documentation is not provided, even in exigent circumstances.

Supervisors of personnel utilizing the CALEA collection system 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 within 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 health and safety issues with the CALEA collection system or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy mitigate the risk of impartial and biased law enforcement. The CALEA collection system is only used after court authorization has been granted, or situations evidencing exigent circumstances. The CALEA collection system does not use any biometric measurement technology.

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.