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 depending on the authorization, 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 that were previously used to conduct a variety of 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 all these functions.

Additionally, the CALEA collection system replaces the physical devices that were 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 artificial intelligence, machine learning, 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 a warrant 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 order is obtained to use the CALEA collection system to covertly monitor telephone calls, SMS, MMS, and network traffic.

An NYPD investigator first obtains court authorization allowing for the use of the CALEA collection system to aid an ongoing investigation. The warrant is obtained with the aid of the prosecutor with proper jurisdiction. The warrant must contain a finding of probable cause by a judge, as well as an explicit authorization for use of the CALEA collection system for a specified period of time.

However, the CALEA collection system may be utilized without first obtaining a 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.

Even if exigent circumstances exist, the NYPD investigator must first document the nature of the emergency before being granted access to the CALEA collection system. Additionally, a court order must be obtained soon-thereafter by the NYPD investigator with the aid of the prosecutorial entity with proper jurisdiction.

Access to the CALEA collection system is critically limited. The NYPD Technical Assistance Response Unit (TARU) must first be provided with all proper documentation which is then 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 furtherance of investigations.

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.

**SAFEGUARDS & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

TARU only grants temporary access to the CALEA collection system. Once access is granted, the investigator is authenticated through a unique username and password. Access is only provided to the CALEA collection system after submitting all proper documentation to TARU. CALEA collection system access only lasts for as long as the court authorization allows, or as long as the exigent or emergency circumstances persist.

The CALEA collection system does not reside on the NYPD computer network. It is a closed system solely used in connection to the operation of the CALEA collection system.

The CALEA collection system may only be used by NYPD personnel during the course of their lawful duties. 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 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 restrictions based on storage capacity.
Data obtained by the CALEA collection system may be 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.

Information contained within NYPD case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Access rights within NYPD case management systems are limited based on lawful duty. Records contained within NYPD computer and case management systems may be used for legitimate law enforcement purposes or official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings.

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;

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.
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 information 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 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 artificial intelligence, machine learning, or 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.