INTERNET ATTRIBUTION MANAGEMENT INFRASTRUCTURE: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that internet attribution management infrastructure 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 internet attribution management infrastructure capabilities.	Added language describing how internet attribution management infrastructure compliments other NYPD technologies.
Expanded upon internet attribution management infrastructure rules of use.	Added language clarifying internet attribution management infrastructure rules of use.
Expanded upon internet attribution management infrastructure safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to internet attribution management infrastructure when job duties no longer require access.
Expanded upon internet attribution management infrastructure data retention.	Added language to reflect NYPD obligations under federal, state and local record retention laws.
Expanded upon internet attribution management infrastructure external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

INTERNET ATTRIBUTION MANAGEMENT INFRASTRUCTURE REVISION

Date of Revision	Description of Revision
February 4, 2026	This impact and use policy was revised to comply with the recently passed amendment to the POST Act, Local Law 56 of 2025.

ABSTRACT

Through its continued growth and availability, the internet makes information more accessible across the world and is intertwined in the daily lives of billions of people. Just as these constantly evolving technological advances provide end users with personal benefits, they also provide new environments for criminal activity to occur. As a result, the New York City Police Department (NYPD) utilizes internet attribution management infrastructure to provide its personnel with the capability to safely, securely, and covertly access the internet in this dynamic environment in furtherance of public safety.

The NYPD produced this impact and use policy because internet attribution management infrastructure includes equipment, software, and systems that may be used to collect, retain or process audio, video, location or similar information.

CAPABILITIES OF THE TECHNOLOGY

The internet works through the exchange of information between networks and devices. For example, the Internet Protocol (IP) address connected to the device being used to view the website must be shared so that the contents of the website can be routed to the device for viewing. Further, in order track the internet activities of visitors, personalize content, and save information about a user, the website may send a "cookie" to the browser on the device used to access the website.

Over time, activities on the internet and the pieces of information left behind from those activities accumulate, resulting in what has been referred to as a "digital footprint" that is capable of identifying an individual user, as well as detecting human versus non-human internet traffic. For a member of the public, the content of a digital footprint may make the difference between whether a website grants immediate access to information or requires additional user authentication. For law enforcement, the content of a digital footprint may make the difference between whether a target of a criminal investigation detects the police affiliation of an undercover officer, placing their life and safety in jeopardy.

The NYPD uses internet attribution management infrastructure, including Ntrepid, to manage digital footprints and allow its personnel to safely, securely, and covertly conduct investigations and detect possible criminal activity on the internet.

The types of equipment utilized by the NYPD for its internet attribution management infrastructure include computer servers, internet lines, switches, modems, and routers, virtual private networks, remote desktop software, desktop and laptop computers, tablets, and smartphones from a variety of manufacturers.

The information that is ultimately accessible to NYPD personnel utilizing this equipment is limited to publicly available information or the information that is viewable as a result of the privacy settings, privacy practices, and access limitations of an internet environment (e.g., chatrooms, social media profiles, messaging applications) or subject of investigation.

The NYPD does not use its internet attribution management infrastructure to obtain unauthorized access to electronic devices, and this infrastructure does not use any biometric measuring

technologies. NYPD internet attribution management infrastructure does not use facial recognition technology and cannot conduct facial recognition analysis.[1]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD internet attribution management infrastructure 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 internet attribution management infrastructure to obtain unauthorized access to electronic devices. NYPD internet attribution management infrastructure may only be used by NYPD personnel for legitimate law enforcement purposes or other official business of the NYPD.

Internet attribution management infrastructure may be used in any situation the supervisory personnel responsible for oversight deems appropriate. The underlying facts are considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purposes or other official business of the NYPD to utilize the technology in a given circumstance.

Court Authorization: The NYPD does not seek court authorization to use internet attribution management infrastructure. Internet attribution management infrastructure allows NYPD personnel to access the internet to view publicly available information and engage in undercover activity to covertly obtain information in investigations in a manner that does not violate the law.

Additional Guidelines: If an NYPD investigation involving political activity requires the use of the internet attribution management infrastructure, the Intelligence Division will use it in compliance with Department policies. The Intelligence Division is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Revised *Handschu* Guidelines.

As with all NYPD operations, no person will be the subject of police action 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 internet attribution management infrastructure will subject employees to administrative and potentially criminal penalties.

Addendum Obligation: 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 internet attribution management infrastructure.

[1] However, a still image obtained using the technology may be used as a probe image for facial recognition analysis. For additional information on facial recognition, please refer to the facial recognition impact and use policy.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Physical Safeguards & Security Measures: The equipment used by the NYPD for internet attribution management infrastructure is kept within NYPD facilities and/or stored in locations that are inaccessible to the public. NYPD personnel seeking access to the equipment and associated contents of internet attribution management infrastructure are authenticated by username and/or password. A supervisor must periodically account for the equipment used for internet attribution management infrastructure.

Data Safeguards & Security Measures: Access to NYPD internet attribution management infrastructure is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to internet attribution management technologies is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

This information obtained by using internet attribution management infrastructure is retained within an NYPD computer or case management system. Only authorized users have access to this information. 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 is 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 computer and case management 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 from 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

Information obtained by using internet attribution management infrastructure may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigation, and disciplinary proceedings. Information relevant to an investigation is stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management 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 NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. The retention period of a "case investigation record" depends on its classification and 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 they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought.

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 data collected by the NYPD through its use of internet attribution management infrastructure pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of the law.

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by NYPD's use of internet attribution management infrastructure.

If the NYPD obtains material related to a criminal case by using internet attribution management infrastructure, 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 information 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 will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community concern.

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.

Vendors & Contractors: The NYPD purchases internet attribution management infrastructure and associated equipment or 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 internet attribution management infrastructure 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 information obtained using NYPD internet attribution management infrastructure 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 within 24 hours. The NYPD must make reasonable efforts to notify individuals affected 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 publicly available online.

TRAINING

NYPD personnel utilizing internet attribution management infrastructure receive command level training on the proper operation of the technology and associated equipment. NYPD personnel must use internet attribution management infrastructure in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of internet attribution management infrastructure, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing internet attribution management infrastructure 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 tests or reports regarding the health and safety effects of the NYPD's internet attribution management infrastructure. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of the internet attribution management infrastructure.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that NYPD's internet attribution management infrastructure is used effectively and responsibly. The NYPD does not believe that this technology is being used in a manner that disparately impacts any protected groups as defined in the New York City Human Rights Law.

The safeguards and audit protocols built into this impact and use policy for NYPD internet attribution management infrastructure mitigate the risk of partial and biased law enforcement. Internet attribution management infrastructure is only capable of accessing information made available to NYPD personnel on the internet. Internet attribution management infrastructure does not use any biometric measurement technologies. Based on these safeguards, any theoretical risks of NYPD's internet attribution management infrastructure are effectively mitigated and do not result in disparate impacts.

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. Should an officer initiate enforcement action against a person, 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 only race, age, and gender, but other identifying characteristics or information.