TRANSACTION INTERCEPT TOOL: IMPACT AND USE POLICY

DATED: DECEMBER 1, 2025

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update

ABSTRACT

The New York City Police Department intends to utilize a transaction intercept tool ("Transaction Intercept") to protect children from sex trafficking and sexual exploitation. Transaction Intercept is a rules-based chatbot that utilizes natural language processing to respond with pre-written, human generated responses when it is contacted by individuals in publicly accessible online environments who are attempting to communicate with children in connection with sexual activity. While these individuals believe that they are communicating with children, they will in fact be communicating with Transaction Intercept. This will enable the Department to intercept sexual predators and build criminal cases against them.

The Department produced this impact and use policy because Transaction Intercept may collect, retain, and share images and location metadata received from individuals who communicate with it.

CAPABILITIES OF THE TECHNOLOGY

The Department will utilize Transaction Intercept, developed by non-profit organization Street Grace, to support the Department's efforts to investigate and deter the commercial sexual exploitation of minors.

Transaction Intercept enables Department personnel to select parameters to create "personas" that appear to be minors. Each persona is assigned a phone number through the Transaction Intercept platform. The Department will then create decoy advertisements, including the persona's assigned phone number and place them on websites associated with sex trafficking and commercial sexual exploitation activities. An individual seeking to engage in these activities (a "Potential Buyer") can respond to these advertisements. Once a Potential Buyer initiates contact, the assigned persona (which is, in reality, Transaction Intercept) will respond. The Potential Buyer and Transaction Intercept will then message each other.

Transaction Intercept does not use publicly available language models with self-learning capabilities nor does it generate content. Instead, it operates through a proprietary hybrid conversational language-understanding feature that uses a custom-built language model. This model analyzes and interprets incoming messages and matches them to a set of pre-written phrases informed by consultation with members of law enforcement.

Transaction Intercept can engage in conversations with multiple Potential Buyers simultaneously. Department personnel can monitor all ongoing conversations via Transaction Intercept's platform interface, which allows real-time oversight and the ability to take over any conversation at any time. If probable cause is established, the Department will take steps to arrest the Potential Buyer.

The Transaction Intercept platform is incapable of independent outreach. In other words, Transaction Intercept never initiates contact with any Potential Buyer and only responds once a Potential Buyer contacts the persona in the decoy advertisement. Transaction Intercept is programmed to avoid introducing references to sexual services or money unless such topics are first raised by the Potential Buyer.

Transaction Intercept retains data shared with it by Potential Buyers, including messages, images, and location metadata. If a Potential Buyer sends images, such as photographs, Transaction Intercept will retain those images for 30 days and then delete them. Other data is retained indefinitely. Data in the Transaction Intercept platform cannot be altered.

Transaction Intercept does not collect any audio or biometric data and does not employ facial recognition technology. However, if a potential buyer provides an image via Transaction Intercept, that image may be used as a probe image for facial recognition analysis, consistent with applicable Department policy.[1]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

Transaction Intercept 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.

Transaction Intercept may only be used by NYPD personnel for legitimate law enforcement purposes. Authorization for use must be granted by supervisory personnel responsible for oversight. Only members of the service who are authorized and have received proper training are permitted to operate Transaction Intercept or engage with individuals through the platform.

Court Authorization: The NYPD does not seek court authorization before using Transaction Intercept, as there is no reasonable expectation of privacy in these interactions. Transaction Intercept operates solely on publicly accessible websites and all interactions are voluntarily initiated by a Potential Buyer.

Additional Guidelines: Transaction Intercept is not used for investigating political activity. NYPD investigations involving political activity are conducted by the Intelligence Division, which is the sole entity in the NYPD that may conduct investigations involving political activities pursuant to the *Handschu* Consent Decree.

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 Transaction Intercept 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 Transaction Intercept tools.

[1] For additional information on facial recognition, please refer to the facial recognition impact and use policy.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Data Safeguards & Security Measures: Access to Transaction Intercept is limited to NYPD personnel with an articulable need to use the technology in connection with the investigations described above. Transaction Intercept is accessed through its secure platform, and its data is encrypted. Authorized users must be authenticated by a username and password before accessing the Transaction Intercept platform. Access to Transaction Intercept is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

The NYPD can export data, such as conversations and images, from Transaction Intercept's platform. This data is then retained within the appropriate NYPD case management system. Only authorized users have access to the 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 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

Data is retained on the Transaction Intercept platform and can be exported into the applicable case management systems as needed. Messages are retained indefinitely on the Transaction Intercept platform. Images are retained on the Transaction Intercept platform for thirty days and then are automatically deleted, unless exported into the applicable case management systems.

Data 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. Relevant data will be 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 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.

The misuse of any data associated with Transaction Intercept 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 Transaction Intercept pursuant to the New York State Freedom of Information Law. The NYPD will review and respond to such requests in accordance with the applicable provisions of the law.

EXTERNAL ENTITIES

Data relevant to a criminal case will be turned over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the data to the defendant(s) in accordance with criminal discovery laws.

No external entities will have access to the Department's Transaction Intercept records. Transaction Intercept includes a feature that allows participating law enforcement agencies to view and enter notes into their platform associated with a specific phone number. While other agencies may choose to use this feature, the Department will not enter or share any notes in this system. The Department will, however, retain the ability to view notes entered by other agencies.

Other law enforcement agencies may request data 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 data to partnering law enforcement and city agencies in connection with 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.

Vendors & Contractors: The NYPD obtained Transaction Intercept 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 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 may have access to NYPD's data on Transaction Intercept, including the associated software environment as needed for system maintenance, infrastructure updates, and data backfilling, 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. Additionally, Transaction Intercept requires written consent for each instance of a vendor and/or their contractor accessing the Department's account related to provision of the technology and maintenance thereof.

Vendors and contractors are legally obligated by contract 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 Transaction Intercept 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

Only NYPD personnel who have completed approved training are authorized to use Transaction Intercept. NYPD personnel receive command level training, in coordination with Street Grace, on the proper operation of the technology.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing Transaction Intercept are responsible for security and proper utilization of the technology. 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 purpose 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. In addition, the Transaction Intercept platform includes a comprehensive audit log that records access and data export activity, including the identity of the user and the time of access.

HEALTH & SAFETY REPORTING

There are no known tests or reports regarding the health and safety effects of Transaction Intercept. 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 Transaction Intercept.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that Transaction Intercept is used effectively and responsibly. The NYPD does not believe that this technology has shown any potentially disparate impacts on any protected groups as defined in the New York City Human Rights Law.

Transaction Intercept is deployed strictly for investigative purposes and only with supervisory approval. Additionally, Transaction Intercept cannot initiate conversations. All conversations are voluntarily initiated by a Potential Buyer responding to a decoy advertisement. The NYPD restricts access to authorized personnel, and all activity including message content, access, and data exportation, is logged and subject to audit. Transaction Intercept does not use any biometric measurement technologies and does not collect or analyze biometric data.

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.