SOCIAL NETWORK ANALYSIS TOOLS:
IMPACT & USE POLICY

ABSTRACT

Social network analysis refers to reviewing, processing and, when appropriate, retaining accessible information on social networking platforms (e.g., Facebook, Twitter, and Instagram). To support public safety, the New York City Police Department (NYPD) uses social network analysis tools to automate this process with publicly available information viewable on social networking platforms.

The NYPD produced this impact and use policy because social network analysis tools are capable of reviewing, retaining, and processing audio, video images, location, or similar information contained on social networking platforms.

CAPABILITIES OF THE TECHNOLOGY

NYPD social network analysis tools process information on social networking platforms to aid personnel in discovering information relevant to investigations and to address public safety concerns.

For example, in the aftermath of a terrorist attack committed outside of New York City, the NYPD may use social network analysis tools to quickly assess the social media profile of the perpetrator for connections to the New York City area and allocate resources in response.

Similarly, social network analysis tools assist the NYPD in addressing criminal activity in New York City. When investigating an assault committed by multiple subjects, social network analysis tools can reveal investigative leads by highlighting otherwise unknown connections between the subjects acting in concert.

However, the NYPD may miss information critical to investigations because users can easily remove information posted on social media and social media platforms routinely delete content and deactivate accounts for violations of terms of service. Accordingly, social network analysis tools allow the NYPD to retain information on social networking platforms relevant to investigations and alert investigators to new activity on queried social media accounts.

Information accessible to NYPD personnel using social network analysis tools is limited to publicly available information, or information that is viewable as a result of user privacy settings or practices.

Social network analysis tools cannot be used for computer hacking, and the tools do not use artificial intelligence, machine learning, facial recognition, or any other biometric measuring technologies.
SOCIAL NETWORK ANALYSIS TOOLS: 
IMPACT & USE POLICY

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD social network analysis tools policy seeks to balance the public safety benefits of this technology with individual privacy. The NYPD must use social network analysis tools 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.

Information identified by using social network analysis tools does not by itself establish probable cause to arrest or obtain a search warrant. However, it may generate leads for further investigation.

Social network analysis tools may only be used for legitimate law enforcement purposes relating to the official business of the NYPD.

The NYPD does not seek court authorization prior to using social network analysis tools. The processed information is limited to publicly available information or information that is viewable as a result of user-selected privacy settings or practices.

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 social network analysis tools.

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 activity 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 social network analysis tools will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Access to social network analysis tools is critically limited. Authorized users are authenticated by username and password. Account credentials for social network analysis tools must be securely maintained and stored at all times.

Information obtained from NYPD social network analysis tools relevant to an investigation is stored within an appropriate case management or computer systems. 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.
The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. All NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory authentication. The active directory 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 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. Members of the NYPD 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 to any system will subject employees to administrative and potentially criminal penalties.

**POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA**

Information obtained from social network analysis tools relevant to a case or investigation is stored electronically in an appropriate NYPD case management and computer systems. 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 computer and case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Information 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 system 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 social network analysis tools pursuant to the 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

If the use of social network analysis tools yields information relevant to a criminal case, the NYPD will share it with the prosecutor with jurisdiction over the matter. Prosecutors will provide the information 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 the information or details related to it 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.

Following the laws of the State and City of New York, as well as NYPD policy, the information related to social network analysis 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.
SOCIAL NETWORK ANALYSIS TOOLS:
IMPACT & USE POLICY

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 social network analysis tools 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 social network analysis tools 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

NYPD personnel using social network analysis tools receive command level training on the proper operation of the technology and associated equipment. All NYPD personnel must use social network analysis tools in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing social network analysis tools 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 social network analysis tools or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD social network analysis tools mitigate the risk of impartial and biased law enforcement. Social network analysis tools are only capable of processing information a user chooses to share on social networking platforms. NYPD social network analysis tools do not use artificial intelligence, machine learning, facial recognition, or any other 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.