DIGITAL FORENSIC ACCESS TOOLS:
IMPACT & USE POLICY

ABSTRACT

While advancements in encryption technology benefit the individual privacy of end users, the same advancements present new and difficult challenges for law enforcement. Even when law enforcement obtains a court ordered search warrant, encryption may make effecting a search impossible. As a result, the New York City Police Department (NYPD) utilizes digital forensic access tools to extract and search encrypted or inaccessible data from electronic devices.

The NYPD produced this impact and use policy because digital forensic access tools includes equipment and software that may be used to collect, retain, process, or share audio, video, location, or similar information from electronic devices.

CAPABILITIES OF THE TECHNOLOGY

The NYPD uses both physical devices and software as digital forensic access tools. The physical devices are used to extract information (e.g., communications, photographs, videos, etc.) from electronic devices, and software is used to process the information contained on those devices.

Digital forensic analysis tools also allow NYPD personnel to maintain the integrity of the evidence obtained from electronic devices, and establish a clear chain of custody for that information.

The information that is ultimately accessible to NYPD personnel utilizing this equipment is limited to the information contained on an electronic device.

The NYPD does not use its digital forensic access tools to engage in unauthorized access or “hacking” of electronic devices. Digital forensic access tools do not use artificial intelligence, machine learning, facial recognition, or any other biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD digital forensic access tools policy seeks to balance the public safety benefits of this technology with individual privacy. Digital forensic access tools 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 digital forensic access tools to engage in unauthorized access or “hacking” of electronic devices.

Digital forensic access tools are used with court authorization in the form of a search warrant. 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 a search of the electronic device where digital forensic access tools may be used.

Digital forensic access tools may also be used in the absence of court authorization with individual consent or if exigent circumstances exist. If exigent circumstances exist, an NYPD investigator

DRAFT FOR PUBLIC COMMENT:
POSTED JANUARY 11, 2021
Digital Forensic Access Tools: Impact & Use Policy

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.

Supervisory personnel must be consulted prior to use of digital forensic access tools. The underlying facts are considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purpose to utilize the technology in a given circumstance.

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 digital forensic access 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 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 digital forensic access tools will subject employees to administrative and potentially criminal penalties.

Safeguard & Security Measures Against Unauthorized Access

Digital forensic access tools are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the equipment. Access to associated software is limited to authorized users who are authenticated by username and password.

Information obtained by using digital forensic access tools 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.

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.

Draft for Public Comment:  
Posted January 11, 2021
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. 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**

Information obtained by using digital forensic access tools 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.

Information stored within NYPD computer and case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Information 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.

The misuse of any information will subject employees to administrative and potentially criminal penalties.
MEMBERS OF THE PUBLIC MAY REQUEST INFORMATION OBTAINED FROM NYPD USE OF DIGITAL FORENSIC ACCESS 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

IN THE EVENT THE NYPD IS UNABLE TO ACCESS INFORMATION EXTRACTED FROM ELECTRONIC DEVICES USING DIGITAL FORENSIC ANALYSIS TOOLS DUE TO COMPLEX ENCRYPTION AND DEVICE SECURITY, THE NYPD MAY MAKE THE DEVICE ACCESSIBLE TO CERTIFIED DIGITAL FORENSIC EXPERTS OF THE PRIVATE VENDOR OF THE TECHNOLOGY TO OBTAIN THEIR ASSISTANCE IN ACCESSING THE INFORMATION.

IF DIGITAL FORENSIC ACCESS TOOLS OBTAIN 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 MATERIAL 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 MATERIAL 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.

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 digital forensic access 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 digital forensic access 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 utilizing digital forensic access tools receive command level training on the proper operation of the technology and associated equipment. NYPD personnel must use digital forensic access tools in compliance with NYPD policies and training.

**INTERNAL AUDIT & OVERSIGHT MECHANISMS**

The use of digital forensic access tools, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing digital forensic access 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.
DIGITAL FORENSIC ACCESS TOOLS:
IMPACT & USE POLICY

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 digital forensic access 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 digital forensic access tools mitigate the risk of impartial and biased law enforcement. Digital forensic access tools are only capable of accessing information contained on a specific electronic device. Digital forensic analysis tools are only used by NYPD personnel after obtaining a court ordered search warrant, individual consent, or under exigent circumstances. Digital forensic access 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.