CRIMINAL GROUP DATABASE: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that the criminal group database does not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence or machine learning.
Expanded upon the criminal group database capabilities.	Added language clarifying the criminal group database capabilities. Added language describing how the criminal group database compliment other NYPD technologies.
Expanded upon the criminal group database rules of use.	Added language clarifying the criminal group database rules of use.
Expanded upon the criminal group database safeguard and security measures.	Added language regarding information security. Added language to reflect the removal of access to the criminal group database when job duties no longer require access.
Expanded upon the criminal group database data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon the criminal group database external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

Information and intelligence gathering is a critical component of modern policing and an invaluable tool for detectives investigating crime. In support of its mission of reducing violent crime and protecting the public, the New York City Police Department's (NYPD) Criminal Group Database provides investigators with information about alleged gang members and additional intelligence relating to street gangs.

The NYPD produced this impact and use policy because the criminal group database is capable of sharing audio data and both still and video images with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Often referred to as the "Gang Database," the NYPD Criminal Group Database is used as an investigative resource to maintain consistent, up-to-date intelligence regarding criminal groups and street gangs. Based in an NYPD case management system, the Criminal Group Database efficiently centralizes vital criminal group related intelligence that would otherwise be kept throughout different isolated data compartments within the NYPD.

Information such as criminal group names, associated incidents, geographic data, inter-criminal group dynamics and relationships, and alleged criminal group membership, including lawfully-obtained photographs, aliases, addresses, known associations, is consolidated in such a way that NYPD investigators are able to discern trends, relationships, and patterns to enhance public safety, criminal investigations, and resource allocation.

Subjects cannot be entered into the NYPD Criminal Group Database automatically; inclusion data must be manually inputted into the database. If a person is fingerprinted by law enforcement, inclusion in the database does not appear in a person's criminal history or record of arrest. The NYPD Criminal Group Database cannot be accessed through the NYPD Domain Awareness System (DAS[1]). However, if DAS is used to search for information connected to a person included in the criminal group database, that inclusion will appear along with the name of the criminal group.

The Criminal Group Database does not use any biometric measuring technologies. The NYPD Criminal Group Database does not use facial recognition technologies and cannot conduct facial recognition analysis. However, still images within the database may be used as a probe image for facial recognition analysis.[2]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD Criminal Group Database policy seeks to balance the public safety benefits of this technology with individual privacy. The Criminal Group Database 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

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

Entry into the database is not proof of criminal behavior, it is simply an investigative lead. Entry alone is not grounds for a stop, arrest, or any other enforcement action. The database can only be accessed by limited authorized NYPD personnel. NYPD personnel may only access the database for legitimate law enforcement purposes.

A subject can be included in the Criminal Group Database in one (1) of two (2) ways. The first way involves some form of acknowledgement of criminal group membership, by either: 1a) a self-admission of criminal group membership to a member of the NYPD; 2a) being identified as a member of a criminal group by two independent and reliable sources; or 3a) social media posts admitting to membership in a criminal group.

The second way requires two (2) of the following to be true: 1b) frequent presence at a known criminal group location; 2b) possession of criminal group-related documents; 3b) association with known criminal group members; 4b) social media posts with known criminal group members while possessing known criminal group paraphernalia; 5b) scars and tattoos associated with a particular criminal group; or 6b) frequent wearing of the colors and frequent use of hand signs that are associated with particular criminal groups. A subject will only be included in the Criminal Group Database if these actions are deemed a consistent course of conduct.

A subject must be recommended for entry prior to their inclusion in the Criminal Group Database. Only a limited number of NYPD personnel can recommend a subject be entered into the database: a precinct field intelligence officer; an investigator assigned to a Detective Bureau Gang Squad; or an investigator assigned to Social Media Analysis and Research Team.

A written narrative and supporting documentation must be provided with the recommendation for Criminal Group Database entry. This recommendation is reviewed by a supervisor in a Detective Bureau Gang Squad who will either approve or reject the recommendation, or request additional analysis by the NYPD Gang Analysis Section before making a decision.

Subjects included in the Criminal Group Database are reviewed every three (3) years, and on the subjects' twenty-third (23rd) and twenty-eighth (28th) birthdays to determine if their actions and records warrant continued inclusion. Additionally, the NYPD has a mechanism for self-initiated review at any time. Once a subject is removed from the database, the fact that they once were affiliated with a criminal group is permanently hidden from the database and NYPD computer systems.

Court authorization is not required to use the Criminal Group Database. The Criminal Group Database only contains lawfully obtained information previously collected by NYPD personnel.

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 the Criminal Group Database.

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 Criminal Group Database will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

The Criminal Group Database is confidential-password-protected and access is restricted to only authorized users. Access to the database is limited to personnel who have an articulable need for access in furtherance of lawful duty, relating to the official business of the NYPD. Authorization must be requested by a Commanding Officer, and approved by the Information Technology Bureau (ITB).

Access to the Database is limited to authorized users who are authenticated by username and password. Database access is limited to NYPD personnel with an articulable need to use the database in furtherance of a lawful duty. Access to the Criminal Group Database is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

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 are 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

The Criminal Group Database 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. Authorized users are authenticated by username and password.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[3] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[4]

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.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal

[3] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[4] *See* NYC Charter 3003.

information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of relevant case investigation record.

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 related to the NYPD Criminal Group Database 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 relevant to a criminal case, information is turned over to 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 Criminal Group Database from the NYPD in accordance with applicable laws, regulations, and New York City and NYPD policies. The NYPD may provide information contained with the database 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. Affirmation that a subject is included in the NYPD's Criminal Group Database may be shared with other law enforcement agencies in the course of conducting joint gang/criminal group investigations.

Information from the Criminal Group Database is not shared with the New York City Housing Authority or employers conducting background checks. Further, consistent with local law and NYPD policy, the Department does not share information in the database with Immigration and Customs Enforcement to conduct immigration enforcement, initiate deportation proceedings, or affect visa applications or citizen applications.

Following the laws of the State and City of New York, as well as NYPD policy, information contained in the database 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, members of the NYPD 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 Criminal Group Database 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 Criminal Group Database 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 contained within the database 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 as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected 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 publically available online.

TRAINING

NYPD personnel using the NYPD Criminal Group Database receive command level training on the proper operation of the technology and associated equipment. NYPD personnel must operate the database in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Only a limited number of NYPD personnel can recommend a subject be entered into the database; only a precinct field intelligence officer, an investigator assigned to a Detective Bureau Gang Squad, or an investigator assigned to the Social Media Analysis and Research Team may recommend a subject be entered into the database. This formal recommendation requires a written narrative and supporting documentation that justify database inclusion. Recommendations are reviewed by a supervisor in a Detective Bureau Gang Squad who will either approve or reject the recommendation, or request additional analysis by the Department's Gang Analysis Section.

Subjects included in the Criminal Group Database are reviewed every three (3) years, and on the subjects' twenty-third (23rd) and twenty-eighth (28th) birthdays to determine if their actions and records warrant continued inclusion. Additionally, the NYPD has a mechanism for self-initiated review at any time. Once a subject is removed from the database, the fact that they once were affiliated with a criminal group is permanently hidden from the database

Supervisors of personnel who have access to the Criminal Group Database 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.

Immutable audit logs are created when any information is searched or accessed through the NYPD Criminal Group Database. The log-in and use of the system is traceable to a particular user and periodically audited for misuse by the precinct or unit's Commanding Officer. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

All members of the NYPD are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by 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 health and safety issues associated with the NYPD Criminal Group Database or the associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into the impact and use policy for the NYPD Criminal Group Database mitigate the risk of impartial and biased law enforcement. The Criminal Group Database is an investigative resource to maintain consistent, up-to-date intelligence regarding criminal groups and street gangs. The Criminal Group Database efficiently centralizes vital criminal group related intelligence that would otherwise be kept throughout different isolated data compartments within the NYPD. The Criminal Group Database does not use any biometric measuring technologies.

Critics have asserted that inclusion in the Criminal Group Database disparately impacts people of color and has significant collateral consequences. Entry into the Criminal Group Database is not proof of criminal behavior, it is only an investigative lead. Entry alone is not grounds for a stop, arrest, or any other enforcement action. Moreover, New York State does not permit civil gang injunctions such as those routinely utilized in other jurisdictions. Unlike many states, New York does not have a sentencing enhancement for gang/criminal group members, nor a statute that criminalizes gang/criminal group membership. A subject’s presence in the NYPD Criminal Group Database simply does not have the collateral consequences comparable to other jurisdictions.

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.