EXHIBIT B

FACIAL RECOGNITION: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that facial recognition software 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 facial recognition capabilities section.	Added language clarifying facial recognition capabilities. Added language how facial recognition is not integrated with other NYPD technologies. Added language describing the photo repository.
Expanded upon facial recognition rules of use.	Added language clarifying facial recognition rules of use. Added language describing facial identification; the human review of potential possible match candidates.
Expanded upon facial recognition safeguard and security measures.	Added language regarding information security. Added language to reflect the removal of access to facial recognition technologies when job duties no longer require access.
Expanded upon facial recognition data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon external entities section.	Added language to reflect the NYPD's obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

Facial recognition is a digital technology the New York City Police Department (NYPD) uses to compare probe images to the NYPD arrest photo gallery for specific legitimate law enforcement purposes. Used in combination with human analysis and additional investigation, facial recognition technology is a valuable tool in solving crimes and increasing public safety.

The facial recognition used by the NYPD is routinely evaluated by the National Institute of Standards and Technology (NIST) for efficiency and accuracy. NYPD facial recognition investigators are trained, and access to the technology itself is limited solely to those personnel. No one has ever been arrested solely based on facial recognition results by the NYPD.

The NYPD produced this impact and use policy because the facial recognition technology processes biometric information.

CAPABILITIES OF THE TECHNOLOGY

Since 2011, the NYPD has successfully used facial recognition technology to investigate criminal activity and increase public safety. The NYPD uses facial recognition to aid in the identification of suspects whose images have been recorded on-camera at robberies, burglaries, assaults, shootings, and other serious crimes. The NYPD also uses facial recognition to aid in the identification of persons unable to identify themselves (e.g., persons experiencing memory loss or unidentified deceased persons).

NYPD investigators often obtain video and photo over the course of an investigation. If a video or photo contains an image of a face of an unknown individual, the image can be submitted for facial recognition analysis in accordance with NYPD facial recognition policy.

Known as a probe image, NYPD facial recognition software compares the image to a controlled and limited group of photos already within lawful possession of the NYPD, called the photo repository. The photo repository only contains arrest and parole photographs of individuals that have been charged with a crime where criminal court has jurisdiction. Probe images are never entered into and do not become part of the photo repository.

NYPD facial recognition technology analyzes one probe image at a time. The software generates a pool of possible match candidates that are manually reviewed by specially trained NYPD facial recognition investigators to determine the differences and similarities between a probe image and a potential match.

The NYPD does not integrate facial recognition technology with any NYPD video cameras or systems (e.g., CCTV cameras, unmanned aircraft systems, and body worn cameras, etc.) for real-time facial recognition analysis. The NYPD does not have a capability for real-time facial recognition.

Facial recognition technology does not use any additional biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD facial recognition policy seeks to balance the public safety benefits of this technology with individual privacy. Facial recognition technology 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 facial recognition process does not by itself establish a basis for a stop, probable cause to arrest, or to obtain a search warrant. However, it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

Facial recognition technology must only be used for legitimate law enforcement purposes. Authorized uses of facial recognition technology are limited to the following:

1. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime;
2. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;
3. To identify a deceased person;
4. To identify a person who is incapacitated or otherwise unable to identify themselves;
5. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification; or
6. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

For criminal investigations, a possible facial recognition match serves as a lead for additional steps. An arrest will not be made until the assigned investigator establishes, with other corroborating evidence, that the suspect identified as a possible match is the perpetrator in an alleged crime.

When an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, the investigator must submit a request for facial recognition analysis. Specifically, the request is made for the image depicting the face of the unknown person (the probe image) to be compared to photos in the NYPD arrest and parole photo repository. The request for facial recognition analysis must include a case or complaint number for the matter under investigation and the probe image(s) of the unidentified person.

The facial recognition investigator must confirm the basis of the request is in compliance with the enumerated list authorized uses of facial recognition technology. That confirmation must be documented by the requesting investigator in an appropriate NYPD case management system. The facial recognition investigator will select a probe image of the unidentified person from the submitted images. If image quality is unsuitable for facial recognition comparison, the requesting investigator will be notified and given the opportunity to submit additional images.

The facial recognition investigator will run a search using a facial recognition software for comparison of the probe image to images lawfully obtained by the NYPD. The software generates a pool of possible match candidates.

If a possible match candidate is identified, the facial recognition investigator must then manually review and analyze each result. This process, known as facial identification, consists of visual comparison of the facial characteristics of each candidate against the probe image. Comparisons are made with regard to various facial features such as the eyes, ears, nose, mouth, chin, lips, eyebrows, hair/hairline, scars, marks, and tattoos. A detailed background check is conducted by the facial recognition investigator to corroborate a possible match.

Next, a possible match candidate is submitted for peer review by other facial recognition investigators. A supervisor of the facial recognition investigator performs a final review of a possible match candidate and provides final approves, if appropriate.

If there is a difference of opinion with the findings, the supervisor will direct personnel to continue investigation for a possible match candidate. A report of negative results will be provided to the requesting investigator if a possible match candidate is not identified or approved by the supervisor.

If a possible match candidate is approved, the facial recognition investigator will prepare a possible match report and attach it to the requesting investigator's case file in the case management system. The possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Images obtained from body-worn cameras worn by NYPD officers are not routinely submitted for facial recognition analysis. For example, the NYPD does not use facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

The NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies.

The NYPD does not seek court authorization prior to the use of facial recognition technology since the tool conducts analysis of images that have been lawfully-obtained by the NYPD.

The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Detectives or Deputy Commissioner, Intelligence and Counterterrorism.

In situations where use of a NYPD facial recognition technology has not been foreseen or prescribed in policy, the Chief of Detectives or Deputy Commissioner of Intelligence and

Counterterrorism, will decide if use is appropriate and lawful. 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 facial recognition technology.

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 facial recognition technology will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Access to facial recognition technology is limited to NYPD facial recognition investigators. Access to facial recognition technology is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when facial recognition investigators are transferred to a different command).

Facial recognition investigators using the software are first authenticated by username and password. Facial recognition investigators are provided with access only after completing mandatory training related to use of the technology.

Information resulting from use of facial recognition technology is retained within NYPD computer and case management 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. 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 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 results of facial recognition analysis 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. Facial recognition analysis results relevant to a case or investigation are stored in appropriate NYPD computer or case management systems. These results 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.

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.[1] 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.[2]

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

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

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 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 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 information obtained from the NYPD use of facial recognition technology 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 facial recognition technology produces information related to a criminal case, the NYPD will turn it 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 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. Such 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 stemming from facial recognition technology 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;
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 facial recognition technology 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 facial recognition technology associated program 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 facial recognition data 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 utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of facial recognition technology, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing facial recognition technology 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 health and safety issues with facial recognition technologies or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for facial recognition technology mitigate the risk of impartial and biased law enforcement. NYPD facial recognition policy integrates human investigators in all phases. All possible facial recognition matches undergo a peer review by other facial recognition investigators. Further, the possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asians Americans, women, and groups other than non-white males. However, an important federal government study on the subject noted that in "hybrid machine/human systems," where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers.

Facial recognition technology utilizes algorithms in order to identify possible match candidates to a probe image. The NYPD only uses facial recognition algorithms which have been evaluated by the National Institute of Standards and Technology (NIST) for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for facial recognition are periodically updated as necessary based on subsequent NIST evaluations.

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.