IRIS RECOGNITION: IMPACT & USE POLICY

ABSTRACT

Since 2010, the New York City Police Department (NYPD) has successfully used iris recognition technology exclusively to verify that arrestees are being arraigned in connection to the correct case. Prior to implementation of the technology, there were at least six (6) incidents where an arrestee pretended to be a different arrestee in order to be arraigned on a lesser offense. Since the implementation of the iris recognition program, no such incidents.

The NYPD produced this impact and use policy because iris cameras capture images of a person’s iris, and the associated software processes this biometric information.

CAPABILITIES OF THE TECHNOLOGY

A human iris contains over one-hundred (100) more data reference points than a human fingerprint. Like fingerprints, iris textures are randomly created during embryonic gestation, and the chance of false matches is very low. Even identical twins have different iris textures. Iris recognition is not affected by clear contact lenses.

Iris images are high resolution photographs of the pigmented portion of an eye. NYPD iris cameras create iris images within seconds. There is no contact between the arrestee and the iris camera. NYPD personnel hold the iris camera between six (6) to eight (8) inches away from the arrestee’s eyes. There is no flash built into the iris cameras.

An iris image is taken upon an arrestee’s entry to central booking, located in each borough, and is automatically compared to an iris image taken just before a live, in-court arraignment by iris recognition software. Within seconds the iris recognition software notifies NYPD personnel of a verified match, mismatch, or an error.

Iris cameras are different from retinal scans. The iris cameras utilized by the NYPD capture high-quality close-up images depicting the pigmentation, striations, and individual markings of an iris. A retinal scan measures the unique patterns on a person’s retina. The NYPD does not use any retinal scanning technologies.

The iris cameras do not photograph any facial features other than eyes. Iris recognition devices and software do not use artificial intelligence, machine learning, facial recognition, or any additional biometric measuring technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD iris recognition policy seeks to balance the public safety benefits of this technology with individual privacy. Iris 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.
IRIS RECOGNITION:
IMPACT & USE POLICY

Because iris recognition technology is used solely to verify arrestee identities prior to a live in-court arraignment, an iris is only photographed if an arrest is being processed “live”; e.g., the arrestee will be arraigned before a judge. No iris photographs are taken if an individual is receiving a desk appearance ticket (DAT) or summons.

In order for an iris image to be taken, arrestees must provide their consent. Failure or inability to capture an iris image will not materially delay arraignment. Iris images are first taken when an arrestee is transferred into the custody of the NYPD Criminal Justice Bureau (CJB) during the Central Booking intake process. A photograph is generally taken of both irises, and the iris images are linked to the arrest number associated with the arrestee.

Immediately prior to an arrestee’s entry into a courtroom for a live arraignment, a second iris image will be created. First, NYPD personnel assigned to operate the iris recognition software enters the arrest number of the arrestee into the software; so the system knows what image to use for the comparison. Next, a photograph is taken of one (1) of the arrestee’s eyes. The iris recognition software automatically compares the iris images taken upon entry to Central Booking to the newly created iris image. The software notifies the NYPD personnel of a verified match, mismatch, or an error. In the event of consecutive errors, an arrestee’s identity can be manually confirmed by the associated arrest photograph prior to entry into the arraignment court.

Similar to the taking of photographs and fingerprints during the arrest process, court authorization is not necessary prior to the NYPD use of iris recognition technology.

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 iris recognition technology.

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

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Iris cameras and computers containing iris recognition software are kept in a secure location, inaccessible to the general public. Additionally, a supervisor must periodically inspect and account for iris cameras.

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
IRIS RECOGNITION: 
IMPACT & USE POLICY

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 NYPD computer systems, 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 to any system will subject employees to administrative and potentially criminal penalties.

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

While an arrestee is awaiting arraignment, members of the NYPD Photo Unit and supervisory members of CJB may access the arrestee’s iris images. Iris images become inaccessible to nearly all NYPD personnel once the arrestee is arraigned. However, iris image metadata, such as date and time of iris recognition confirmation, is interwoven into records maintained by the NYPD Online Prisoner Arraignment Database (ZOLPA).\(^1\) The data maintained by ZOLPA is often the subject of civil litigation and disciplinary proceedings, and therefore, must be retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Information is not used in furtherance of immigration enforcement.

Only select NYPD Information Technology Bureau (ITB) administrators may access the database, and may only do so for maintenance purposes; such as, if the system goes offline unexpectedly. Iris images are inaccessible to all other NYPD personnel, and cannot be used for any subsequent investigatory purposes.

NYPD personnel utilizing computer systems are authenticated by username and password. Access to NYPD computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD computer systems are further limited based on lawful duty.

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

\(^1\) ZOLPA is primarily used for routine NYPD administrative purposes, and therefore, is excluded from the POST Act definition of surveillance technology.
IRIS RECOGNITION:
IMPACT & USE POLICY

computer systems may be used for legitimate law enforcement purposes or official business of the
NYPD.

The misuse of any data 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 on NYPD iris 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

The NYPD purchases iris 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 iris recognition technology 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.

No additional entities outside the NYPD have access to the iris images.

TRAINING

NYPD personnel using iris recognition technology receive command-level training administered
by the Criminal Justice Bureau on the proper operation of the technology and associated
equipment. NYPD personnel must operate iris recognition technology in compliance with NYPD
policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing iris recognition technologies are responsible for security and
proper utilization of the technology and associated equipment. Supervisors are directed to inspect
IRIS RECOGNITION: IMPACT & USE POLICY

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).

NYPD policy requires authorized users to maintain the confidentiality of accessible information and forbids improper dissemination of information, access beyond authorization granted by the NYPD, and breach of confidentiality.

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all information coming into 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 iris recognition technology or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for iris recognition mitigate the risk of impartial and biased law enforcement. Iris recognition technology is only used to confirm the identity of arrestees upon their entry into a courtroom for a live arraignment. The iris cameras do not photograph any facial features other than eyes. Iris recognition cameras and software do not use facial recognition, artificial intelligence, or machine learning 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.