ABSTRACT

The New York City Police Department (NYPD) uses license plate readers (LPRs) to help NYPD personnel locate stolen or wanted vehicles, vehicles connected to AMBER alerts, Silver alerts, missing persons reports, abductions reports, and vehicles connected to other crimes. Within seconds, LPRs can notify NYPD personnel that a queried license plate has passed within the device’s range, allowing NYPD investigators to take immediate action in furtherance of public safety.

The NYPD produced this impact and use policy because LPRs are capable of capturing images of license plate numbers on passing vehicles, identifying the location of the vehicle at the time of recording, and sharing that information with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

LPRs are specialized cameras that quickly capture images of license plate numbers affixed to vehicles that pass within the LPRs sensory range. An internal processor then converts the image of the license plate into a text the computer can process. This text is automatically compared against administrative databases containing enumerated lists of license plates of interest (i.e. stolen, wanted, etc.). LPRs are capable of properly functioning day or night, and in a variety of weather conditions.

NYPD makes use of two (2) kinds of LPRs: stationary and mobile. Stationary LPRs are permanently affixed to a specific location and record the license plates of all vehicles that pass within the LPR range. Mobile LPRs are attached to various NYPD vehicles and use the same technology to capture images of license plates the vehicle passes as it moves. NYPD officers operating a NYPD vehicle imbedded with a NYPD tablet1 will receive an alert if the LPR scans a vehicle of interest, such as a vehicle reported stolen. NYPD LPRs cannot be used to track a vehicle in real-time.

Both stationary and mobile LPRs record a vehicle’s license plate number and state of issuance, an images of a the vehicle and the license plate, and the date, time and location the vehicle passed the LPR.

NYPD LPRs do not use artificial intelligence, machine learning, or any biometric measurement technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD LPR policy seeks to balance the public safety benefits of this technology with individual privacy. LPRs 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 NYPD tablets, please refer to the Portable Electronic Device impact and use policy.
Court authorization is not sought prior to NYPD use of LPRs. Motor vehicles are heavily regulated by the government. The field-of-view of the LPRs utilized by the NYPD is strictly limited to public areas and locations. LPRs capture images of license plates that are readily observable to any member of the public.

NYPD personnel may only use LPRs to execute their lawful duties, relating only to official business of the NYPD. LPRs do not by themselves establish probable cause for an arrest, but provide NYPD investigators with valuable leads. The NYPD limits authorized use of LPRs to the following circumstances:

1. Routine vehicle patrol;
2. Creation of alerts for specified complete or partial plate numbers; and
3. Capture movement of specified complete or partial plate numbers that momentarily pass the device.

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 LPRs.

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 LPRs will subject employees to administrative and potentially criminal penalties.

**SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

LPR data is accessible by using the NYPD Domain Awareness System (DAS)\(^2\). Access to DAS is limited to authorized users who are authenticated by username and password. Access rights within DAS are 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

\(^2\) For additional information on DAS, please refer to the DAS impact and use policy.

---

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

Data recorded by LPRs is accessible through DAS. All NYPD authorized users may only access DAS to execute their lawful duties by making official inquiries, which relate only to official business of the NYPD. Historical searches of LPR data may be conducted:

1. To determine if specified complete or partial plate numbers were detected by one or more fixed or mobile LPRs;
2. To identify all complete plate numbers detected by one or more fixed LPR during a specified time period;
3. To identify all complete plate numbers detected by a mobile LPR mounted on one or more specified vehicles during a specified time period;
4. To identify all complete plate numbers detected within a specified area during a specified time period; and
5. To identify preceding or subsequent complete plate numbers associated with one or more specified complete or partial plate numbers detected by one or more fixed or mobile LPRs in order to identify possible associates.

Data collected through the NYPD’s use of LPRs is retained for five (5) years.

LPR data that is relevant to a criminal is stored electronically in an appropriate NYPD computer or case management system. 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.

Data stored within NYPD computer and case management systems are retained in accordance with applicable laws, regulations, and New York City and NYPD policies. Recordings 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 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 data obtained from the NYPD’s use of LPRs 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 a LPR obtains data related to a criminal case, the NYPD will turn the data over to the prosecutor with jurisdiction over the matter. Prosecutors will provide this data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may LPR data from NYPD in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide LPR data 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.

Authorized agents within the state of New Jersey (NJ) have limited access to the NYPD LPR recorded data. Authorized agents of NJ law enforcement agencies are capable of conducting a search for pings of a specific license plate against NYPD owned or accessed LPR readers. However, NJ Authorized Agents do not have access to DAS.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from LPR use 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
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 LPRs 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 LPRs 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.
TRAINED

NYPD officers using LPRs receive command level training on the proper operation of the technology and associated equipment. Officers must operate NYPD LPRs in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing LPRs 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.

Any search conducted in DAS relating to LPR associated information is auditable by ITB.

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 NYPD 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 LPRs or associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for LPRs mitigate the risk of impartial and biased law enforcement. LPRs capture images of vehicle license plates utilizing NYC’s public roadways. LPRs 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. Should an officer initiates 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.