ABSTRACT

To help ensure public safety and security, and to detect, deter, and prevent potential terrorist activities, the New York City Police Department (NYPD) coordinated with Microsoft to develop a networked Domain Awareness System (DAS). Today, DAS is not only a tool aiding in the detection and prevention of terrorist attacks; it greatly enhances the quality of criminal investigations and the effectiveness of members of service. DAS allows officers to access critical information relevant to ongoing security and public safety efforts, and boosts the collaborative nature of those efforts by employing the resources of the private sector and other city agencies. DAS is an important part of the NYPD’s integrated approach to providing protection for those who work in, live in and visit New York City.

The NYPD produced this impact and use policy because DAS is capable of sharing video images, location, and acoustic data with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Originally designed as a counterterrorism platform, DAS is now a program that aggregates a substantial quantity of the information NYPD personnel use to make strategic and tactical decisions. DAS is a software that efficiently centralizes vital information that would otherwise be kept throughout different isolated data compartments within the NYPD.

In the field, DAS allows NYPD personnel access to real-time 911 information, past history of call locations, a person’s NYPD arrest history and other relevant information responding officers may need when answering calls. DAS is capable of distributing wanted posters and missing person alerts amongst NYPD personnel, increasing the potential of a timelier recovery, rescue and if appropriate, arrest.

DAS provides officers with critical alerts on any issues or potential threats at queried locations. DAS allows NYPD members to access environmental data, view electronic injury and accident reports, and allows NYPD personnel to search for previously prepared crime complaint reports, domestic violence reports, and other police forms.

The NYPD utilizes Closed Circuit Television (CCTV) cameras throughout the five (5) boroughs. DAS behaves as a centralized repository through which authorized users can access CCTV cameras. NYPD Detectives, Sergeants, and higher ranked members can use DAS to view live feed from CCTV cameras. A limited number of select NYPD personnel with the rank of police officer may be granted CCTV viewing privileges based on the nature of their assignment. DAS cannot be used to download or retain CCTV video.

License plate readers (LPRs) are specialized cameras that quickly capture images of license plate numbers mounted to vehicles that pass within their range-of-view. An internal processor then converts the image of the license plate a text the computer can process. This data, along with the date and time the plates were scanned and the location of the LPR, is automatically stored within

---

1 For additional information on CCTV systems, please refer to the CCTV systems impact and use policy.
2 For additional information on LPRs, please refer to the LPR impact and use policy.
an administrative database. DAS behaves as a centralized repository through which this LPR data can be accessed. The DAS software itself is incapable of reading license plates.

ShotSpotter\(^3\) is a gunfire or gunshot detection system. ShotSpotter captures the time, location, and audio associated with a potential gunfire incident. DAS behaves as a centralized repository through which ShotSpotter data can be accessed. The DAS software itself is incapable of detecting gunshots or gunfire.

DAS does not contain any editing features, and does not have the ability to change the accessible information. DAS does not use artificial intelligence, machine learning, video analytics, facial recognition or any other biometric measurement technologies.

**RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY**

NYPD DAS policy seeks to balance the public safety benefits of this technology with individual privacy. DAS 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.

NYPD personnel may only access the DAS features they have been authorized to view. NYPD personnel must do so only under circumstances required in the execution of lawful duty relating to the official business of the NYPD. Access rights within DAS is limited based on lawful duty.

Court authorization is not necessary in order to use DAS. DAS is software that centralizes lawfully obtained data and information that would otherwise be kept isolated in different data compartments within the NYPD.

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 DAS.

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 DAS will subject employees to administrative and potentially criminal penalties.

**SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS**

DAS is confidential-password-protected and access is restricted to only authorized users. Authorized users consist only of NYPD personnel in various commands, whose access has been requested by their commanding officer, and approved by the Information Technology Bureau (ITB).

---

\(^3\) For additional information on ShotSpotter, please refer to the ShotSpotter impact and use policy.
If relevant to an investigation, information contained within DAS features may be downloaded and retained in an appropriate NYPD computer or case management system. Only authorized users have access to 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 related to the official business of the NYPD.

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 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**

DAS efficiently centralizes vital information that would otherwise be kept throughout different isolated data compartments within NYPD computer systems. Authorized users can use DAS to download various NYPD records into computer or case management systems that are relevant to an investigation such as complaint reports, arrest reports, Intergraph Computer Aided Dispatch (ICAD) call data, and ShotSpotter and LPR data.

CCTV video cannot be downloaded by the vast majority of DAS users. To retain CCTV video, NYPD personnel must make a request for retention to the NYPD Lower Manhattan Security Initiative (LMSI). Only LMSI personnel are capable of downloading CCTV video.
DOMAIN AWARENESS SYSTEM (DAS):
IMPACT & USE POLICY

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 is 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.

POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request information related to DAS 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

External stakeholders providing NYPD with access to their public-space facing cameras have the ability to designate one of their own employees as their stakeholder representative. Stakeholder representatives only have access to their own public-space facing CCTV camera(s). Stakeholder representatives do not have access to any of the searchable databases accessible within DAS, ShotSpotter, LPR readings, or any other technology contained within DAS.

Stakeholders and stakeholder representatives must agree to NYPD confidentiality and privacy guidelines. Stakeholders and stakeholder representatives are informed that use of NYPD computer systems beyond authorized access, or for personal or non-NYPD business matters is strictly prohibited. Stakeholder representatives who are found in violation of this policy are notified that they will be subject to a termination of assignment.

The information accessible through DAS is often connected to a criminal investigation. Where an arrest occurs, the NYPD will turn any such relevant data 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 data accessible through DAS from the NYPD in accordance with applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide data accessible through DAS 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.
Following the laws of the State and City of New York, as well as NYPD policy, information taken
from DAS 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. However, unless they are an external-stakeholder, community leaders, civic
organizations and members of the news media do not have direct access to any DAS CCTV video
or any of the searchable databases within the system.

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 DAS 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 DAS 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
contracts 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**

All recruits attending the NYPD Academy receive training on the proper operation of DAS and its associated equipment. NYPD personnel receive additional command level training on accessible DAS features. All NYPD personnel must use DAS in compliance with NYPD policies and training.

**INTERNAL AUDIT & OVERSIGHT MECHANISMS**

Immutable audit logs are created when any information is searched or accessed through DAS. 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.

Supervisors of personnel utilizing DAS 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.

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 ITB.
HEALTH & SAFETY REPORTING

There are no known health and safety issues attributable to DAS or its associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for DAS mitigate the risk of impartial and biased law enforcement. DAS is a program that centralizes a large quantity of lawfully obtained data, information and resources to aid NYPD personnel in making tactical and strategic decisions. DAS does not use artificial intelligence, machine learning, video analytics, 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.