ELECTROMAGNETIC WEAPONS DETECTION SYSTEM:

DRAFT IMPACT AND USE POLICY FOR PUBLIC COMMENT

Posted March 28, 2024

ABSTRACT

Electromagnetic weapons detection systems can distinguish weapons from personal items. Unlike the use of traditional metal detectors, individuals do not need to be separated from their belongings or slow their pace as they walk through the system.

The New York City Police Department (NYPD) produced this draft impact and use policy because the NYPD intends to conduct a pilot program using an electromagnetic weapons detection system equipped with video cameras to help prevent individuals from bringing weapons into the transit system. The video cameras are part of a real-time image-aided alert system that indicates the presence of a potential weapon to NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

The electromagnetic weapons detection system operates similarly to other high-traffic automated weapons detection systems already used by sports stadiums and arenas, entertainment and hospitality venues, and healthcare facilities. The system emits ultra-low frequency, electromagnetic pulses; the frequency is in the same range as anti-theft systems widely deployed in retail settings for loss prevention. These pulses pass through objects moving through the electromagnetic weapons detection system. System sensors process the relayed information and the electromagnetic weapons detection system uses this data to determine if it detects a potential weapon.

The electromagnetic weapons detection system is equipped with cameras. If the system detects a potential weapon or weapons being worn or carried by an individual, the system will capture a still image and an approximately three second video of the individual moving through the system. The system will alert the NYPD that a potential weapon has been detected, and wirelessly transmit the still image and video to a tablet being monitored by an NYPD officer. A cube will appear on both the still image and video clip, indicating the location of the potential weapon being worn or carried by the individual. The location of a cube is discerned by the system based on the electromagnetic data processed by the system sensors.

The system also uses an alert tagging feature that will help the NYPD record the cause of an alert. If the system notifies the NYPD of a potential weapon, the monitoring officer will be required to use the alert tagging feature to memorialize what caused the alert. If a potential weapon is not detected by the electromagnetic weapons detection system as an individual passes through the system, no still or video images will be transmitted to the monitoring officer.

Individuals can carry normal personal items with them through the screening process, as well as personal bags and backpacks. If an individual walks at a normal pace, the entire scanning process takes less than three seconds. Due to their composition and shape, some non-weapons may be detected as a potential weapon. If the system alerts the NYPD of a potential weapon, but a weapon is not found in the area indicated by the cube, then the individual will be permitted to enter the transit system.

The electromagnetic weapons detection system being considered by the NYPD does not utilize biometric measuring technologies. It does not use facial recognition technologies and cannot conduct a facial recognition analysis.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The electromagnetic weapons detection system must be used in a manner consistent with the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

Only a Department executive at the rank of Captain or above can designate a transit entrance as the location for an electromagnetic weapons detection system checkpoint. The checkpoint supervisor will determine the frequency of passengers subject to inspection (for example, every fifth passenger or every tenth passenger). The frequency should be based on the volume of passengers, available police personnel on hand to perform inspections, and the flow of commuter traffic in the selected location. The checkpoint supervisor may increase or decrease the frequency of inspections based on commuter traffic. However, the location of the checkpoint and the frequency of passenger inspections must be recorded in the checkpoint supervisor's activity log.

NYPD personnel assigned to the checkpoint will be required to advise individuals that their entry to the transit system is subject to screening by the electromagnetic weapons detection system. Anyone may refuse to be screened by the electromagnetic weapons detection system and elect not to enter the transit system. A refusal to be screened by the system will not constitute probable cause for an arrest or reasonable suspicion for a stop. However, an individual will not be permitted access to the transit system if that individual refuses to be screened by the electromagnetic weapons detection system.

If the electromagnetic weapons detection system alerts the NYPD of a potential weapon, NYPD personnel will divert the individual with the potential weapon from the flow of traffic and conduct a search of the area or areas indicated by cubes in the system. The monitoring officer will be required to use the alert tagging feature to memorialize what caused the alert. Absent additional information giving rise to reasonable suspicion, NYPD personnel are prohibited from frisking or searching areas not outlined by a cube in the electromagnetic weapons detection system.

In accordance with guidance published by the United States Food and Drug Administration (FDA), the NYPD will post signs notifying the public that an electronic security system is in use in a visible location in front of the electromagnetic weapons detection system. The signage will be visible prior to an individual's entry into the monitoring area. This signage will alert individuals who have implanted medical devices or other health concerns so that they can decide if they need alternative screening. If an officer is notified by the individual that they are in need of alternative screening, the NYPD will make alternative screening available to that individual.

The NYPD is deploying the electromagnetic weapons detection system pursuant to the special needs doctrine under the Fourth Amendment and will not seek court authorization in connection with its use.

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 electromagnetic weapons detection system will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

When not in use, the electromagnetic weapons detection system will be securely stored by the NYPD in a location inaccessible to the public. Additionally, a supervisor will be required to periodically inspect and account for all aspects of the system. Access to the electromagnetic weapons detection system will be strictly limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Officers' access to the system will be removed when access is no longer necessary for them to fulfill their duties, such as when personnel are transferred to a command that does not use the technology.

Both video and still images recorded by the electromagnetic weapons detection system are encrypted when they are sent to the tablet being used by the monitoring officer and when they are on the tablet. The system does not upload recorded images or videos to a cloud-based system. The vendor of the electromagnetic weapons detection system is not able to view any still images or video recorded by the system.

If an alert is relevant to a criminal matter, the still image, video clip, cube or cubes and tag or tags associated with the alert will be downloaded and retained within an appropriate NYPD computer or case management system. Only authorized users have access to NYPD computer or 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 from 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

If an electromagnetic weapons detection system alert is relevant to a criminal matter, the still image, video clip, cube or cubes and tag or tags associated with the alert will be downloaded and retained within an appropriate NYPD computer or case management system. Otherwise, data is automatically deleted on what is known as a first-in-first-out basis; when new data is processed, the oldest system data is deleted to make room for the new data. If an alert and the associated data is not downloaded, it will automatically be deleted on a first-in-first-out basis, or thirty (30) days after the alert was created, whichever is sooner. Once an alert and the associated data is deleted, it cannot be retrieved.

The electromagnetic weapons detection system being considered by the NYPD will only be permitted to be used for legitimate law enforcement purposes or other official business of the NYPD. 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 computer and case management systems are further limited based on lawful duty.

The NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. 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.

The misuse of any data associated with the electromagnetic weapons detection system alert will subject employees to administrative and potentially criminal penalties.

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

Members of the public will be able to request data associated with the NYPD's use of the electromagnetic weapons detection system 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 an alert is relevant to a criminal matter, the NYPD will turn any still image, video clip, cube or cubes and tag or tags associated with the alert over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request data associated with an electromagnetic weapons detection system contained in NYPD computer and case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide data associated with an electromagnetic weapons detection system or information related to it 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, electromagnetic weapons detection system alerts, data associated with alerts, or information related to it, 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 is being made to another City agency or agencies and 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; or
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 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 the electromagnetic weapons detection system, as well as 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 a still image or video obtained through the NYPD's use of the electromagnetic weapons detection system 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 that use the electromagnetic weapons detection system will receive specialized command level training on the proper operation of the technology and associated equipment. NYPD personnel will be required to use the electromagnetic weapons detection system in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Supervisors of personnel utilizing the electromagnetic weapons detection system will be 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

The electromagnetic weapons detection system emits ultra-low frequency, electromagnetic pulses. The frequency of these pulses is in the same range as electronic anti-theft systems widely deployed in retail settings for loss prevention. Implanted electronic medical devices may be affected by electromagnetic radiation emitted from devices that operate in this range.[1] The FDA has determined that the likelihood of electronic anti-theft systems interfering with implanted medical devices is extremely low, and any effects on the implant and the wearer have been found to be transient and unlikely to cause clinically significant symptoms. At the same time, the FDA concluded that individuals with implanted medical devices should be notified when extremely low frequency radio wave systems are in use.[2]

A manual screening alternative will be made available for anyone who has health concerns.

[1] American Heart Association Journal, Circulation; Effects of External Electrical and Magnetic Fields on Pacemakers and Defibrillators: From Engineering Principles to Clinical Practice; Beinart, Roy M.D. and Nazarian, Saman M.D., December 2013.
[2] U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Electronic Product Devices Branch, Division of Enforcement III, Office of Compliance; Guidance for Industry, Labeling for Electronic Anti-Theft Systems; August 2000.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The protocol for the use of the electromagnetic weapons detection system—in particular, the determination before the system is deployed at a particular station at what frequency passengers will be directed through the system—mitigates the risk of a disparate impact resulting from the use of the system.

The electromagnetic weapons detection system will not be connected to any NYPD databases. The electromagnetic weapons detection system does not utilize biometric measuring technologies, does not use facial recognition technologies, and cannot conduct a facial recognition analysis.

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.