SPRINGFIELD POLICE DEPARTMENT

☒ DEPARTMENT DIRECTIVE ☐ DIVISION DIRECTIVE		DIRECTIVE NUMBER 22-039	**OPS 08**
☒ GENERAL ORDER ☐ NOTICE ☐ SPECIAL ORDER ☐ LEGAL NOTICE			ISSUE DATE 05/22/22
SUBJECT: AUTOMATED LICENSE PLATE READER	DISTRIBUTION A, B	REVISION DATES	EFFECTIVE DATE 05/22/22
	REFERENCES:		RESCINDS: NEW

I. PURPOSE

The purpose of this directive is to provide Springfield Police Department (SPD) personnel with guidelines and principles for the use, collection, access, dissemination, retention and purging of Automated License Plate Reader (ALPR) data to ensure the information is used for legitimate law enforcement purposes only and the privacy, civil rights and civil liberties of individuals are not violated.

II. POLICY

It is the policy of the Springfield Police Department to properly and appropriately utilize the ALPR cameras and system to increase public safety by providing a mechanism to assist in minimizing threats and risk of harm to the citizens and their property. Proper use of the ALPR system will increase Department efficiencies through real time response capability in crimes involving the use of vehicles. The use of the ALPR system will also assist in post-incident investigations.

III. DEFINITIONS

A. ALPR System Administrator: The Commanding Officer of the Field Operations Division will act as the ALPR System Administrator.
B. Automated License Plate Reader (ALPR): Any device that automatically scans the license plates of vehicles and using machine learning, interprets the alphanumeric values of the plate.
C. Automated License Plate Reader System: A system that includes ALPR hardware and software that processes license plate images in full or partial to index scanned license plates into a data system for searching and retrieval.
D. Law Enforcement Purposes: The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons, vehicles involved in criminal activity, or hit and run crash investigations.

IV. PROCEDURES

A. The procedures for SPD will ensure the proper use of the ALPR system for the protection of the people of the City of Springfield and their property, while maintaining the highest respect for the privacy, and civil rights and liberties of those whose data is collected by the ALPR system.

1. ALPR devices and information contained within the ALPR databases will be utilized for law enforcement purposes only.
2. Use of the ALPR system for traffic enforcement, fines, towing, or immigration enforcement is prohibited.
3. The administration, maintenance, and training coordination for the ALPR system is the responsibility of the Chief of Police or his designee.
4. Ground-based ALPR installation locations will be determined by the Department through multi-point crime analysis of current criminal incidents, historical criminal incidents, high-density violent crime areas, intersections with a high number of crashes, and common entrance and egress locations for the City of Springfield. The recommendation of ALPR installation locations must be approved by the Chief of Police or their designee after following a similar analysis of criminal incidents near the proposed installation location.

5. An officer may not detain an individual based on the alert from the ALPR system unless the officer has reasonable suspicion that person is involved in criminal activity.
6. Officers will verify all ALPR activations prior to taking enforcement action. Verification should include the visual inspection of the scanned license plate image regarding the plate letters, numbers, and issuing state. The officer should also verify the plate match of the vehicle in question by also comparing the vehicle make, model and any other descriptors provided in the ALPR alert. Verification may also be assisted through the use of a query on the vehicle registration via the Illinois Law Enforcement Data System (LEADS).
7. Creation and use of internal Springfield Police Department Hot List:

    a. The Department internal Hot List is consider confidential information to the extent permitted by law.
    b. Use and creation of the Department's internal Hot List is limited to members of the Criminal Investigations Division and the Street Crimes Unit.
    c. The Department's Hot List is a list of vehicle registrations where detectives have reasonable suspicion to believe the vehicle is legitimately associated with the commission of a criminal offense, or involved in or planning criminal conduct or activity that presents a threat to any individual or community, or the person sought (owner, regular driver, regular passenger, driver or passenger involved in previous criminal conduct or activity in said vehicle, etc.)
    d. Once a detective has sufficient evidence based on the above, an entry into the Department's internal Hot List may be made only after being approved by the Criminal Investigations Division Lieutenant, or the on duty Watch Command Officer.
    e. Entries into the Department's internal hot List must be of a complete license plate. Partial plate entries are prohibited.
    f. Detectives creating an entry into the Department's internal Hot List shall set the entry to expire in no longer than 30 days from the date of entry. Detectives wishing to extend an entry past 30 days shall extend the entry for another 30 days with permission of the Criminal Investigations Division Lieutenant.
    g. Once the entering detective is made aware their ALPR alert is no longer valid, they should immediately remove the vehicle from the Department's internal Hot List or request or have it removed by the ALPR system administrator.

B Data Security, Access and Privacy

1. The Springfield Police Department will not utilize the ALPR system to seek data on any individual or organization based solely on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.
2. Employees shall not use the ALPR system to target any group or individual in a discriminatory manner or infringe on constitutionally protected activities. This shall not preclude the Chief of Police or the system administrator from releasing general information as to the effectiveness of the ALPR program and other such communication.
3. Access to the ALPR system for the purpose of queries will be granted to all SPD sworn officers and criminal analysts. Use of the ALPR system for queries must be related to an official investigation, personnel complaint, administrative investigation, or criminal investigation. All users that are granted access to the ALPR system will be issued a unique username and password. The use of another employee's username and password is also prohibited. The access rights of terminated employees and/or employees that no longer need access to the ALPR system will be promptly removed.
4. Police Officer user accounts will enable search capability across the SPD ALPR network and other agency ALPR networks from law enforcement agencies that have agreed to ALPR data sharing.
5. Detectives, Street Crimes personnel, and Criminal Analyst's user accounts will match those of Police Officers with the addition of creation and use of SPD internal Hot Lists.
6. When conducting investigative queries into an ALPR database, the requestor is required to enter the case number or CAD number for the incident associated with the case. In addition to the case or CAD number the requestor is required to enter the type of crime associated with the search. This entry will be associated with the search and be visible in the system audit logs. Queries regarding administrative or auditing purposes will be excluded from the requirement to provide a case number.

7. Employees are prohibited from releasing any specific information obtained by ALPR devices that would be considered a personal privacy issue, or create the appearance of one, to non-law enforcement personnel unless required by law. Personnel accessing the ALPR data shall also follow SPD ADM-46, which controls the access, transmission, release, and security of protected information.

C. Data Storage, Retention and Sharing

1. The database retention period for all data collected by SPD ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days. Mass downloading of ALPR data via the ALPR cloud storage system is prohibited.
2. Individual ALPR data records downloaded as part of an active investigation become records of the Department. Individual ALPR records that are downloaded for use in an investigation are subject to disclosure under the Illinois Freedom of Information Ace. However, this does not preclude the Department from withholding said records pursuant to any and all exemptions available to it pursuant to the Illinois Freedom of Information Act. Downloaded records are to be treated as evidence and stored according to Departmental procedures and policy by the ALPR end user. Evidence created through use of ALPR query shall also be included in an officer's/analyst's investigative report.

    a. Any data from the ALPR system which needs to be preserved as evidence shall be directly downloaded from the ALPR program to Evidence.com to be stored as digital evidence.
    b. Any other means of preserving evidence from the ALPR system, i.e. screenshots or photographs, is prohibited.

3. External law enforcement agencies may request a query of SPD's ALPR system as part of an active criminal investigation by the external law enforcement agency. The Department will only share SPD ALPR data for official law enforcement purposes in accordance with Departmental policies and local, state, and federal laws and regulations. If the external agency request produces investigative leads in other jurisdictions, SPD will not provide records from those external agencies to the requesting agency. SPD will then refer the requesting agency to the outside agency where the original documents reside.
4. When practical, and in the absence of exigent circumstances, external law enforcement records should be referred to the Commanding Officer of the Criminal Investigations Division for processing and record keeping.
5. Electronic online sharing of SPD historical ALPR data to external law enforcement agencies that use a compatible ALPR system is permissible, at the direction of the Chief of Police or their designee.
6. At no time is ALPR data allowed to be sold, monetized, shared, or otherwise used for any commercial or non-law enforcement purpose, aside from those required by law.

D. Training

The Department will establish end-user training for those employees provided direct access to ALPR data. ALPR system users will be trained prior to being granted access to the ALPR system. Training will include review of this policy, the requirements and processes of creating and deleting entries into the SPD internal Hot List, appropriate use of ALPR technology and possible penalties for ALPR policy violations.

V. ACCOUNTABILITY

A. Agency user audit reports will be produced and inspected monthly to ensure compliance with this policy. The system administrator will be responsible for conducting the monthly audit and reporting any discrepancies, problems, or misuse to the Chief of Police or their designee. The monthly user audit will also contain anonymized user data and transactional data suitable for release on the Department's web-based Transparency Portal.
B. Any Department member found to be in non-compliance with this policy in their use of the ALPR system will immediately have their access suspended to the ALPR system (if an authorized user) and be subject to the appropriate disciplinary or administrative actions.
C. Any non-Departmental personnel found to have gained unauthorized access will be referred to the appropriate authorities for criminal prosecution, as necessary.

Ken Scarlette, Chief of Police

Reviewed for Legal Sufficiency: Emily Fancher, Assistant Corporation Counsel