INTRADEPARTMENTAL CORRESPONDENCE

December 8, 2020
1.14

TO: The Honorable Board of Police Commissioners

FROM: Chief of Police

SUBJECT: AUTOMATED LICENSE PLATE RECOGNITION USAGE AND PRIVACY POLICY – ESTABLISHED

RECOMMENDED ACTION

It is recommended that the Board of Police Commissioners REVIEW and APPROVE the policy regarding the usage and privacy policy of the Automated License Plate Recognition.

DISCUSSION

The attached Special Order establishes Department Manual Section 3/568.53, *Automated License Plate Recognition Usage and Privacy Policy.*

Should you have additional questions regarding this matter, please contact Director Lizabeth Rhodes, Office of Constitutional Policing and Policy, at (213) 486-8730.

Respectfully,

MICHEL R. MOORE
Chief of Police

Attachment

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO.

SUBJECT: **AUTOMATED LICENSE PLATE RECOGNITION USAGE AND PRIVACY POLICY – ESTABLISHED**

PURPOSE: Automated License Plate Recognition (ALPR) technology is a valuable tool for law enforcement and serves to enhance public safety when used appropriately. As with any law enforcement capability, ALPR technology shall be used in a manner consistent with the United States Constitution, the Fourth Amendment, and other applicable statutory authorities. The purpose of this Order is to establish procedures to ensure that all activities pertaining to the capture, use, retention, and dissemination of information obtained through the ALPR System complies with all applicable federal, state, and local laws.

PROCEDURE: **AUTOMATED LICENSE PLATE RECOGNITION USAGE AND PRIVACY POLICY – ESTABLISHED.** Department Manual Section 3/568.53, *Automated License Plate Recognition Usage and Privacy Policy*, has been established and is attached.

AMENDMENT: This Order adds Section 3/568.53 to the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

MICHEL R. MOORE
Chief of Police

Attachment

DISTRIBUTION "D"

DEPARTMENT MANUAL
VOLUME III
Revised by Special Order No. , 2020

568.53 AUTOMATED LICENSE PLATE RECOGNITION USAGE AND PRIVACY POLICY. *The Department's Automated License Plate Recognition System (ALPR) System is a computerized database resulting from the operation of one or more mobile or fixed cameras ("ALPR Cameras"). When combined with computer algorithms, the ALPR System reads and conveys images of license plates and the characters they contain into computer-readable data. The data collected by the ALPR Cameras consists of a photo of the vehicle license plate, the date, time, and location the photo was taken, and the identification number of the ALPR Camera capturing the information. The ALPR System records and stores data from license plates only. When used effectively and in accordance with the law, the ALPR data can be a valuable tool in solving crimes.*

Authorized Uses. *The ALPR System and the recording of ALPR data shall only be retained, accessed, and used for the following official Department purposes:*

- *Criminal investigations or proceedings;*
- *Non-criminal investigations (e.g., missing and found persons);*
- *Administrative investigations or proceedings (e.g., pursuit and complaint investigations);*
- *Civil investigations or proceedings;*
- *Situational awareness operations; and*
- *Responses to cognizable threats to public safety.*

Limitations on Use of ALPR Data. *The Department's ALPR Cameras shall only be used to collect and record information that is exposed to public view where there is no reasonable expectation of privacy (e.g., vehicle(s) on public roadways or on private property but whose license plate(s) are visible from a public place).*

Moreover, the Department's ALPR System shall only be accessed and used on a "need to know" and "right to know" basis. This means the person accessing the information must have both the lawful authority to receive the information ***and*** *an investigative purpose for the information in order to carry out official responsibilities. The ALPR data shall only be collected, recorded, retained, accessed, and used for official Department-related purposes that are in accordance with this policy and applicable law. Any use of the ALPR System for non-official purposes may subject an employee to discipline and, depending on the misuse, shall result in deactivation of the employee's ALPR account for a period of time. Moreover, an attempt of an improper or actual login by a deactivated employee shall be captured in audit trails and reported to Professional Standards Bureau.*

Persons Authorized to Access and Use the ALPR Data. *There are two type of users authorized to use the ALPR System: ALPR System Administrators and ALPR Data Users. Each type of user is given different access controls, responsibilities, and training.*

ALPR System Administrators – Defined. *Department personnel assigned within Information Technology Bureau (ITB) have the highest access rights to the ALPR System. The ITB is responsible for ensuring the maintenance of the ALPR server, database, application software, and verifying proper operation of the system. The ALPR System Administrators are also responsible for assisting in any reports of inoperability or malfunction of ALPR-equipped vehicles.*

ALPR Data Users – Defined. *Any active Department employees (both sworn and civilian) or independent contractors, who have received written authorization from their supervisor and have been granted permission from ITB to query the ALPR System.*

> ***Note:*** *Employees equipped with the ALPR Cameras in their Department vehicles may receive an ALPR Hit, and when used for this purpose officers receive on-the-job training. They have no ability to add, remove, or change any information in the ALPR System.*

ALPR Data Users Training. *All ALPR Data Users shall complete one of the Department's POST-certified training courses on accessing and using ALPR data prior to querying the ALPR System. A second course is offered as supplemental training for ALPR Data Users on search capabilities.*

ALPR System Administrators. *All ALPR System Administrators shall receive training to fulfill their job responsibilities by a current ALPR System Administrator and/or vendor prior to accessing the ALPR System as an ALPR System Administrator.*

> ***Note:*** *Any ALPR Data User or ALPR System Administrator who has not used their ALPR System account for one year and whose duties require their use of the ALPR System, shall complete a reorientation training course prior to accessing the ALPR System.*

Sharing of ALPR Data. *The ALPR System is a valuable investigative tool and shall be used appropriately in accordance with this policy and the provisions of the law. When sharing information from the ALPR System, Department employees shall do so with integrity and confidentiality. All ALPR data recorded and/or retained by the Department shall not be sold, shared, transferred, or otherwise disclosed for commercial purposes or to persons or entities that are not authorized to record, retain, access or use ALPR data. The ALPR data shall only be shared with other local law enforcement agencies that have an interagency agreement with the Department. All current and future contracts shall be reviewed and contain a clause prohibiting the sharing of Department ALPR data outside of the agency with whom the Department has an agreement.*

Retention and Deletion of ALPR Data. *In general, ALPR data recorded or retained by the Department shall be retained for a period of two years. After two years, ALPR data recorded or retained by the Department will be logically deleted. Logical deletion is the process whereby the data record is flagged in the database when deleted. The ALPR records that have been logically deleted cannot be viewed or accessed by ALPR Data Users and can only be queried by an ALPR System Administrator. All ALPR data shall be permanently deleted after five years, and 24 hours and one minute, with the exception of data needed for prosecutions or administrative hearings that are retained indefinitely upon approval.*

Retaining ALPR Data Beyond the Two-Year Logical Deletion Period for Ongoing Prosecution/Administrative Purposes. *In the event ALPR data is determined to have evidentiary value in a criminal or administrative investigation, the investigator shall submit an Intradepartmental Correspondence, Form 15.02.00, to an ALPR System Administrator requesting that the information be saved beyond the two-year retention period. The written request shall include the Division of Records (DR) Number or case number, the specific reason the data should be retained, and the investigator's contact information. Once the request has*

been approved by the investigator's supervisor, the ALPR System Administrator shall ensure the requested information is retained in the ALPR System until it has been approved for deletion. Every two years, ITB shall verify with the investigating officer if the information is eligible for deletion.

***Note:** Investigating officers are encouraged to keep any related ALPR data hard copies in their case file(s) for court purposes.*

The ALPR data that has been logically deleted will only be searchable under the following circumstances:

- *The investigation is related to a "serious felony" as defined in California Penal Code (PC) 1192.7(c), and/or a "violent felony" as defined in California Penal Code 667.5(c);"*
- *The investigation is related to a violation of 136.1 PC – Intimidation of Witnesses and Victims when it is accompanied by force or by an express or implied threat of force or violence; in furtherance of a conspiracy; with a prior conviction for a violation of this section, or when committed for pecuniary gain;*
- *The investigation is related to a violation of 236.1 – Human Trafficking;*
- *The investigation is related to a violation of 273.6(a) PC – Violation of a Protective Order;*
- *The investigation is related to a violation of 646.9 PC – Stalking;*
- *The investigation is related to a violation of 290(c) PC – Sex Offender Registration;*
- *The investigation is related to terrorist activity, including individuals and groups who plan, threaten, finance, aid/abet, and attempt or perform unlawful acts in furtherance of terrorist activity (refer to Department Manual Section 4/271.46); or,*
- *Pursuant to a court order.*

If the case investigator meets the above criteria and seeks to query ALPR data that has been logically deleted, he or she shall request his or her Commanding Officer (CO) prepare an Intradepartmental Correspondence, Form 15.02.00, documenting the criteria has been met and specifying the ALPR data requested.

The 15.02.00 shall be submitted to the CO of ITB. If the CO of ITB approves the request, he or she will forward the request to an ALPR System Administrator who will complete the search and provide the data requested to the investigator.

***Quality Assurance.** The Department shall make reasonable efforts to assure the accuracy of ALPR data. Department personnel are reminded that ALPR data, by itself, does not establish probable cause to arrest and that further investigation is needed. Additionally, Department personnel shall attempt to verify records obtained prior to conducting an investigative stop.*

Department personnel who discover that an ALPR National Crime Information Center Want contains an verified error, shall immediately notify Communications Division of the release of the vehicle and/or vessel. Communications Divisions shall, without delay, broadcast a cancellation of the want on the vehicle and/or vessel. Patrol officers assigned to Department vehicles equipped with the ALPR Cameras shall attempt to verify the accuracy of the "Hot Lists" data prior to conducting an investigation.

Data Security & Security Breach of Notification. *The ALPR data shall be stored on a Department-approved storage system compliant with standards established by the Federal Bureau of Investigation's Criminal Justice Information System (CJIS). Physical and remote access to the data storage system shall be restricted to authorized persons only. Any Department data storage system approved to store ALPR data shall be physically located on property owned by the City of Los Angeles and/or within California Department of Justice compliant cloud systems. The ITB shall ensure that the management and storage of ALPR data is recorded or retained by the Department.*

The Department shall immediately disclose to the California State Attorney General a breach in the security of ALPR data, once the Department discovers or is notified of such breach of information. If the breach potentially includes data of 500 or more persons, ITB shall submit the applicable forms as required by California Civil Code s. 1798.29(e); and, California Civil Code s. 1798.82(f), to the California State Attorney General (See https://oag.ca.gov/privacy/databreach/report-a-breach for additional details).

Custodian of ALPR System and Records. *The CO of ITB shall be the official custodian of the Department's ALPR system, unless otherwise designated by the Department. The ITB shall be responsible for ensuring that the operation, management, and maintenance of the ALPR System is in accordance with the procedures and guidelines set forth in this policy and applicable law.*

> ***Note:*** *Whenever an ALPR System Administrator or an ALPR Data User separates from the Department, their user account in the ALPR System shall be promptly deactivated and deleted by ITB.*

The ITB shall ensure that the ALPR System configurations and security features, as well as any ALPR vendor agreements, contain appropriate privacy safeguards and data protections as recommended by the best practices of the CJIS policy of the United States Department of Justice, Federal Bureau of Investigation.

Records of Access and Periodic System Audits. *The ITB shall ensure that a database of records of ALPR end-user activity, including all queries to the ALPR System is maintained. The records of access shall be maintained for at least five (5) years. At a minimum, the records of access shall include all of the following:*

- *The date and time the information is accessed;*
- *The license plate number or other data elements used to query the ALPR System;*
- *The username of the person who accessed the information; and,*
- *The identified authorized purpose for accessing the information.*

The access and use of ALPR data through Department systems shall be subject to review and audit by Audit Division. Audit Division shall conduct periodic audits in accordance with Audit Division's Annual Audit Plan. Audit reports shall be maintained by the Department and accessible for public view indefinitely. Moreover, ITB should regularly conduct inspections on the use and the operations of the ALPR System.

If an officer assigned to an ALPR vehicle identifies an inoperable system, they shall complete a Motor Vehicle Trouble Ticket, Form 11.03.00, to request the system to be repaired.