



Liberty University Police Department

Written Directive: Policy 505 Automatic License
Plate Reader Procedure

Page: 1 of 7

Original Date:

Effective Date:

Revised Date:

12 JUN 26

CALEA Reference:

I. Purpose. The purpose of this policy is to establish uniform procedures for the use of the Automatic License Plate Recognition System by sworn police officers.

II. Policy. The purpose of this policy is to provide sworn police officers with guidelines on the proper use of the Automatic License Plate Recognition (ALPR) system.

III. Definitions.

Audit Trail: All records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the

a. date and time of access;

b. license plate number or other data elements used to query the system;

c. specific purpose, as set forth in subsection D, for accessing or querying the system, including the offense type for any criminal investigation;

d. associated call for service or case number; and (v) username of the person or persons who accessed or queried the system.

Audit Trail Data: All forms of data collected or generated by an automatic license plate recognition system for purposes of producing an audit trail.

Automatic License Plate Recognition (ALPR) Program: A system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data.

Alert/Hit: A read matched to a plate that has previously been registered on a hot list of vehicle plates related to stolen vehicles,

wanted vehicles, or other factors supporting investigation, or which has been manually entered by a user for further investigation.

Fixed ALPR system: ALPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Hot List: License plate numbers and letters of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to hit lists circulated among law enforcement agencies.

Mobile ALPR system: ALPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

Portable ALPR system: ALPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

Private Entity ALPR system: A private entity may be, but is not limited to, homeowner's associations, gated communities, shopping malls, other business establishments, or places of worship. These entities often have information sharing agreements with law-enforcement agencies.

Read: Digital images of license plates and vehicles and associated data (e.g., date, time, and geographic coordinates associated with the image capture).

User: Any individual who is authorized to access information and use the system.

IV. Operations.

A. The use of and/or access to an ALPR system will be used for official law enforcement purposes only and in compliance with Code of Virginia (Va. Code) §2.2-5517. Liberty University Police Department (LUPD) will not use a system for the purpose of interfering with individuals engaged in lawful activities or tracking individuals on the basis of the content of lawfully protected speech. ALPR systems are used to identify vehicles, not persons.

B. Va Code §2.2-5517, section D, provides that a law-enforcement agency may use a system only

1. as part of a criminal investigation into an alleged violation of the Va Code or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed;

2. as part of an active investigation related to a missing or endangered person, including whether to issue an alert for such person, or a person associated with human trafficking; or

3. to receive notifications related to a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate.

4. Misuse: Any access, use, disclosure, retention, or dissemination of ALPR data that is not authorized by law, not consistent with official duties, or not in compliance with agency policy constitutes misuse and will result in disciplinary action.

C. All information necessary for the creation of an audit trail will be entered into the query system data. A law-enforcement agency will not query or download system data unless such data is related to at least one of these purposes. A law-enforcement agency may download audit trail data for purposes of generating audit reports.

D. Non-agency owned or contracted ALPR systems

1. Employees who have access to a non-agency owned or contracted ALPR system will report such access to the ALPR program manager or equivalent.

2. Non-agency owned or contracted ALPR systems include memberships or accounts to private entity ALPR systems or databases.

E. Notification of an Alert

1. A stop of a motor vehicle based on a notification from the system will be consistent with Va. Code §2.2-5517, section M. Notification by a system does not constitute reasonable suspicion as grounds for law enforcement to stop a vehicle. Prior to stopping a vehicle based on a notification, a police officer will:

a. Develop an independent, reasonable suspicion for the stop; or

b. Confirm the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification.

i. This confirmation procedure will be an independent comparison of the ALPR system alert and the corresponding hot list notification.

ii. Law-enforcement officers are encouraged to use radio communication to verify the ALPR system alert.

2. If a law-enforcement officer stops the driver of a motor vehicle, stops and frisks a person based on reasonable suspicion, temporarily detains a person during any other investigatory stop, or makes an arrest where notification received from an ALPR system was

involved, the reporting requirements set forth in VA. Code 52-30.2, section C, will be followed.

E. ALPR Hot Lists

1. The primary use of ALPR data involves the comparison of license plate characters collected by an ALPR system to characters contained on a previously compiled hot list. These hot lists may be compiled by the local, state, or federal law enforcement. These hot lists inform law enforcement which vehicles are of interest and why, alerting the user when such a vehicle is read by an ALPR camera. This can be done in real time or using historical ALPR data.

2. Hot lists will be updated at least once every 24 hours, or as soon as practicable, after such updates become available.

a. The Virginia State Police distributes the NCIC hot list four times daily.

b. LUPD and Liberty University Emergency Communications Center (LUECC) will coordinate directly with the Virginia State Police or through their ALPR vendor, the accuracy and currency of the NCIC hot list.

c. LUPD's operated hot list or manually entered hot-listed license plate(s) will be updated at least once every 24 hours or as soon as practicable, after such updates become available.

d. Manually entered license plate lists will contain at a minimum:

- i. Supporting information regarding why a particular license plate is on a specific hot list.
- ii. Vehicle description (year, make, model, and color)
- iii. Legal reason for entry
- iv. Valid 24-hour contact number of entrant or agency.
- v. valid case number or CAD/incident number

3. LUECC will be responsible for maintaining and updating the ALPR hot list.

F. Training Requirements

1. Employees must attend training before using or accessing the ALPR system.

2. ALPR training should occur biannually and should include the following:

- a. Legal update of relevant ALPR matters
- b. Administrative procedures
- c. Technical procedures

3. LUPD will maintain a record of each employee's completion of ALPR training in the employee training file.

G. System Data Usage - Retention and Sharing

1. System data dissemination, sharing, and disclosure is defined in Va. Code §2.2-5517, section F.

a. This section mandates ALPR system data may not be retained beyond 21 days unless:

b. The system data or the audit trail data is part of an ongoing investigation, prosecution, or civil action

c. Such data will be retained by the law enforcement agency until

(i) the investigation concludes without any criminal charges or

(ii) the final disposition of any criminal or civil matter related to the data, including any direct appeals and any writs of habeas corpus pursuant to Article 3 (§8.01-654 et seq.) of Chapter 25 of Title 8.01 or federal law, in accordance with applicable records retention law and policy.

2. ALPR system data may only be downloaded from the system for purposes described in Va. Code §2.2-5517.

3. ALPR system data may not be sold by its employees or its contracted ALPR vendor(s).

4. System data and audit trail data is not subject to disclosure under the Virginia Freedom of Information Act (FOIA)

5. When releasing ALPR information to another law-enforcement agency, it is important to note that Va. Code §2.2-5517, section A, defines a law-enforcement agency as any agency or entity that employs law-enforcement officers as defined in Va. Code §9.1-101.

V. Administrative Process

A. Internal system auditing will occur at least once every 30 days, by the Administrative Services Sergeant.

1. Internal system audits will be conducted in the

following use areas:

a. Queries Conducted - At least 5% of the total monthly queries conducted should be audited to ensure compliance with Va. Code §2.2-5517, section D, (Reference Va. Code 2.2-5517 Section I. 3).

b. Downloads - At least 5% of the total monthly downloads should be audited to ensure compliance with Va. Code §2.2-5517.

c. Traffic Stops - At least 5% of the total monthly traffic stops conducted as the result of an LPR alarm should be audited to ensure compliance.

d. Agency Sharing - A monthly system audit will verify system settings to ensure compliance with Va. Code §2.2-5517, section F (1).

2. ALPR data and audit trail data will be purged and rendered not recoverable in accordance with Va. Code §2.2-5517, section E.

B. Data Security and Access

1. ALPR data is categorized as "for official use only." Ensuring ALPR data remains secure builds public confidence in this technology. Access control to the administrative profile(s) of the ALPR system will be maintained.

2. All collected data will be maintained on a server that is not connected to, or shared with, other law-enforcement databases.

3. The server will be able to provide an inquiry tool, history tracking, and reporting protocols for the entire ALPR system.

4. The server will provide a secure intranet site or internet site, allowing only approved personnel, password-protected access to collected data.

5. State agency internet and intranet sites must be compliant with existing VITA security standards.

C. ALPR Program Manager

1. The Administrative Services Sergeant will be the designated individual who possesses decision-making authority to manage the ALPR program.

2. The Administrative Services Sergeant will, at a minimum:

a. Stay abreast of current case law and legislation

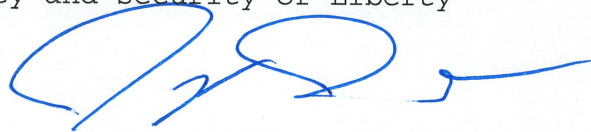
- periodic audits
- b. Monitor the use of the ALPR system and conduct
 - c. Manage user accounts and permissions
 - d. Manage ALPR training
 - e. Updates ALPR policy as necessary

VI. Reporting of Damage. Any loss or damage to the ALPR system will be reported to the Virginia State Police Department of Homeland Security within 24 hours of discovery.

VII. Accountability Statement.

A. No employee of the Liberty University Police Department shall make or distribute to any other individual any copy of this document or part thereof, without the written authorization of the Chief of Police.

B. When situations arise that are not covered by specific instructions, employees shall exercise their best judgment in view of their responsibility for the safety and security of Liberty University.



Colonel Gerald P. Irwin
Chief of Police