Criminal and Juvenile Justice Information Systems Council

CJJIS

Guidelines for the Use of Automated License Plate Readers

Executive Summary

Automated license plate reader (ALPR) technology is being used by law enforcement agencies throughout the nation. Many Florida law enforcement agencies have acquired, or are planning to acquire, ALPR technology. ALPRs assist law enforcement agencies in detection, identification and recovery of stolen vehicles, wanted persons, missing and/or endangered children/adults, and persons who have committed serious and violent crimes. ALPR data can help detectives develop and pursue leads in criminal investigations by assisting in locating suspects, witnesses, and victims by identifying vehicles in the vicinity at the time of the crime.

An ALPR scans, captures, and compares optical license plate information to vehicles associated with crimes or criminals. A match to a license plate results in an alert that notifies law enforcement officers. ALPRs can also store the digital image of the license plate, the time, date, location of the image capture, and the capturing camera information. Stored ALPR data does not include any Personal Identifying Information (PII) of individuals associated with the license plate. Obtaining persons associated with license plate information requires a separate, legally authorized, inquiry to another restricted-access database. Stored data can be used as part of a criminal investigation to determine the location of a known vehicle. An example is when stored LPR data is used to locate a potential route of travel of a vehicle during an AMBER Alert

In the interest of being good stewards and balancing policy and privacy, the Criminal and Juvenile Justice Information Systems (CJJIS) Council, acting pursuant to Section 943.08, Florida Statutes (2013), will issue and adopt uniform statewide guidelines to ensure that ALPRs are used in accordance with substantive procedural safeguards that balance public safety needs and privacy rights.

1. Purpose

a. The purpose of these Guidelines is to provide direction to law enforcement agencies in Florida regarding the use of their ALPRs and ALPR data. These Guidelines are intended to ensure that ALPRs and ALPR-generated data are used only in a manner that is lawful and serves the public interest and fulfill criminal investigative and intelligence needs.

b. These Guidelines should be interpreted and applied to achieve the following objectives:

- the extract stored into the internal memory of an ALPR consists only of information as a result of the license plate capture, such as the image of the license plate, the optical character recognition rendition of the license plate number, the date/time and location of the capture;
- agencies establish protocols for handling alerts to the extracts and that officers respond in accordance with their agency’s policies.

- searching of stored ALPR data is conducted only by authorized persons in furtherance of an active investigation with the safeguarding of individuals' privacy being of paramount concern;

- ALPR data is stored and purged in a defined and secure manner so as to mitigate any potential misuse and improper disclosure of such data.

c. These Guidelines are encouraged for all Florida law enforcement agencies operating under the authority of the laws of the state of Florida that own or operate one or more ALPRs, collect and maintain ALPR data, or receive or are provided access to ALPR data collected by another agency. However, all law enforcement agencies must comply with Florida Statutes governing the use of ALPR data.

2. Policy

a. Every Florida law enforcement agency that uses or possesses an ALPR should implement and enforce a policy that regulates the operation and use of ALPRs and the use, storage, access, and retention of ALPR data. The policy should be consistent with these Guidelines. Specifically, the chief executive will designate appropriate agency personnel to be responsible for administering and overseeing the agency's ALPR program. A designee should be required to ensure that civilian and sworn personnel authorized to use an ALPR or access its data receive proper training in conformity with agency policy, state law, and these Guidelines.

b. ALPRs and data generated by ALPRs shall be used only for a criminal justice purpose.

c. ALPR Scanning Limited to Vehicles Exposed to Public View

- An ALPR may be used only to scan vehicle license plates affixed to public view (i.e., plates of vehicles traveling or parked on any street or highway or other public property, or visible from a place or location at which a law enforcement officer is lawfully present.)

d. Supervisory Approval of ALPR Deployment and Use

- ALPR system use shall be authorized by the chief executive of the agency or his/her designee.

- Authorization may be given for repeated or continuous deployment of an ALPR (e.g., mounting the device on a particular law enforcement vehicle, or positioning the ALPR at a specific stationary location), in which case the authorization shall remain in force and effect unless and until rescinded or modified by the chief executive or his/her designee.

e. Only trained members of a criminal justice agency who are authorized by the chief executive may operate an ALPR

f. Criminal Justice Agency personnel may access or use ALPR stored data only if the person has been designated as an authorized user by the chief executive of the agency or designee, and has been trained by the agency on the proper use of ALPR data.

g. ALPR data may be disclosed by or to a criminal justice agency in the performance of the criminal justice agency's official duties. Any such information relating to a license plate registered to an individual may be disclosed to the individual, unless such information constitutes active criminal intelligence information or active criminal investigative information.

h. ALPR data must be safeguarded in accordance with Florida Statute 316.0777.

3. Definitions and Acronyms

Definitions

a. Automated license plate recognition system. A system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

b. Extract. The files extracted from sources of license plate information such as the Florida Crime Information Center (FCIC) and National Crime Information Center (NCIC) "Hot Files," and DHSMV records including, but not limited to, the expired tag file, expired license file, and sanctioned driver file.

c. Personal identifying information (PII). Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes names, gender, race, date of birth, photographs, addresses, social security numbers, driver's license numbers, or biometric data.

Acronyms

a. ALPR – Automated License Plate Reader (system)

b. CJJIS – Florida Criminal and Juvenile Justice Information Systems (council)

c. CJI – Criminal Justice Information

d. CJIS – Criminal Justice Information Services, a Division of FDLE

e. DHSMV – Florida Department of Highway Safety and Motor Vehicles (agency)

f. FCIC – Florida Crime Information Center (system)

g. FDLE – Florida Department of Law Enforcement (agency)

h. NCIC – National Crime Information Center (system)

i. PII – Personal Identifiable Information

4. Management

a. Strategic Alignment: Agencies deploying ALPR systems should describe in agency policy how the technology aligns and furthers the agency's strategic and tactical deployment objectives.

b. Objectives and Performance: Agencies need to clearly define the objectives for the use of ALPR systems, such as recovery of stolen vehicles, identification of vehicles used in the commission of a crime, etc. and a general strategy for assessing performance and compliance with the agency's policy.

c. Ownership: The hardware and software licenses associated with the ALPR system is the property of the agency, regardless of whether it has been purchased, leased, or acquired as a service, and that all deployments of an ALPR system are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by an ALPR system are the property of the collecting agency, regardless where the data are housed or stored.

d. Classification of Data: ALPR data is protected under Florida Statute 316.0777, whether the data is captured, stored, generated, or otherwise produced by an ALPR system

e. Privacy Impact: ALPR data is protected under Florida Statute 316.0777. Additionally, the International Association of Chiefs of Police published the *Privacy Impact Assessment report for the utilization of license plate readers, September 2009*. Agencies deploying ALPR systems need to consider the privacy risks outlined in this report and include in the ALPR policy, a privacy mitigation strategy that safeguards against potential misuse.

5. Operations

a. Installation, Maintenance, and Support: Agencies shall require regular maintenance, support, upgrades, calibration, and refreshes of an ALPR system to ensure that it functions properly.

b. Deployment: ALPR system use shall be authorized by the chief executive of the agency or his/her designee.

c. Training: Agencies shall require training or other documented proficiency of all personnel who will be managing, maintaining, and/or using an ALPR system. Training should cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.

d. Operational Use: Specific operational factors that must be addressed in deployment and use of an ALPR system:

- The operator should:
  - o Verify that the system has correctly "read" the license plate characters

- Verify the state of issue of the license plate
- If the vehicle hits against an extract record, verify that the record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the hit with the entering agency
- Recognize that the driver of the vehicle may not be the registered owner.

e. Recordkeeping: Agencies should require recordkeeping practices that document all deployments of the ALPR system, including who authorized the deployment; how, when, and where the ALPR system was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage ALPR system implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention

a. Collection: ALPR data will be collected as a by-product of the active scanning of license plates that are compared with the downloaded extract, searched as part of a criminal investigation or in furtherance of a criminal justice purpose. This data is collected by both mobile and fixed ALPR cameras in the same manner. The data is stored in the ALPR system's database. The ALPR database typically contains the image of the license plate, the optical character recognition rendition of the license plate number, the date/time and location of the capture. If additional information is captured and stored, it shall be defined in the agency's policy document. ALPR data will be stored, purged, destroyed or deleted in accordance with Florida Statute 316.0778.

b. Access and Use: ALPR data will be available to Law Enforcement Agency personnel for the tactical enforcement of state statutes for example, identification of a stolen vehicle. ALPR data will be available to Criminal Justice Agency personnel for the purposes of conducting ongoing or continuing criminal investigations and for the purposes of active criminal intelligence operations. Access to ALPR data is authorized by the chief executive of the agency or his/her designee.

c. Information Sharing: ALPR data captured and stored may be shared with other Criminal Justice Agencies for the purposes of conducting ongoing or continuing criminal investigations and for the purposes of active criminal intelligence operations. Agencies shall record the dissemination of ALPR data and notify the recipient of the applicable Florida statutes regarding the privacy restrictions and retention schedules for ALPR data. The sharing of ALPR data shall be authorized by the chief executive of the agency or his/her designee and may be part of a standing order.

d. Security: ALPR systems that do not perform secondary capture of PII or CJI do not need to conform to the FBI CJIS Security Policy (CSP). If an ALPR system performs secondary queries of state and national systems that access PII or CJI, then it shall conform to the FBI CSP. ALPR systems will need to provide user level access based on the role of the person accessing the system (i.e. criminal investigation or criminal intelligence) to ensure the integrity of the systems and confidentiality of the data. The

ALPR system shall be sufficiently designed to minimize the compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data.

e. Data Retention and Use: ALPR data shall be retained in accordance with Florida Statute 316.0778. ALPR data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion may be retained for no longer than 3 anniversary years. Access to ALPR data for criminal investigation or intelligence purposes is limited to authorized Criminal Justice Agency personnel for no longer than 3 anniversary years and requires an agency case number or case name and logging of access. Data captured, stored, generated, or otherwise produced shall be accessible in the ALPR system for 30 days for tactical use.

7. Oversight, Evaluation, Auditing, and Enforcement

a. Oversight: Agencies shall maintain records documenting ALPR use, or ALPR data access and use, whether kept manually or by means of an automated record-keeping system. Agencies shall document in policy a reporting mechanism and a protocol to regularly monitor the use and deployment of ALPR systems to ensure strategic alignment and assessment of policy compliance.

b. Evaluation: Agencies shall annually assess the overall performance of the ALPR system so that it can:

- identify whether a technology is performing effectively;
- identify operational factors that may impact performance effectiveness and/or efficiency;
- identify data quality issues;
- assess the business value and calculate return on investment of a technology; and
- ensure proper technology refresh planning.

c. Auditing: Agencies shall document in policy the manner in which audits will be conducted to include all access to data captured, stored, generated, or otherwise produced by the ALPR to ensure that only authorized users are accessing the ALPR data and establish an annual audit schedule.

d. Enforcement: Agencies shall establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with the Agency's ALPR policy.