AUTOMATIC LICENSE RECOGNITION (ALPR) SYSTEM

Policy Statement

The use of any automatic license plate recognition system (hereafter referred to as ALPR) must be in accordance with § 2.2-5517, *Code of Virginia*.

A fundamental element of policing is locating stolen vehicles or vehicles involved in other criminal acts such as child abduction and drive-by shootings, and non-criminal acts such as missing persons and persons suffering a mental health crisis. ALPR systems play an increasingly important role in public safety by assisting with the location of wanted vehicles and persons while enhancing productivity, effectiveness, and officer safety. The ALPR cameras recognize, read, and compare motor vehicle license plates against various police databases much more efficiently than officers manually scanning and making comparisons while on patrol.

The Powhatan County Sheriff's Office leases access to ALPR cameras through Flock Group Inc., (FLOCK). FLOCK and their customers are responsible for the security, storage and retention of data collected by these systems. The data captured by the system is retained for no longer than 21 days.

Purpose

The purpose of this policy is to set forth guidelines to govern the use of the FLOCK Safety System by the deputies of the Powhatan County Sheriff's Office. The FLOCK Safety System consists of automatic license plate recognition (ALPR) cameras and Vehicle Fingerprint™ technology which allows deputies to identify accurate, objective, and unbiased leads to solve and prevent crimes.

Definitions

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

B. **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.

C. **Hot List**: License plate numbers and letters of stolen vehicles, vehicles owned by persons of interest, and vehicles associated with AMBER and/or other Alerts that are regularly added to hot lists circulated among law enforcement agencies. Hot list information can come from a variety of sources, including information entered in the Virginia Criminal Information Network (VCIN) and the National Crime Information Center (NCIC), including but not limited to national alerts (e.g. Amber, Silver, etc.), Department of Homeland Security watch lists (e.g. terrorists, etc.), missing persons, persons with warrants, stolen vehicles, and stolen license plates. Law enforcement agencies can also interface their own, locally compiled hot lists to the ALPR system. These lists serve an officer safety function as well as an investigatory purpose. In addition to the agency's supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if a vehicle license plate involved in an investigation is read by the ALPR system.

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

E. **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.

F. **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.

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

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

I. **ALPR Program Manager**: The Investigations Lieutenant and/or other designee who is responsible for the security, training, auditing, user access (activating and deactivating user accounts), and reporting of ALPR use and effectiveness to the Sheriff and/or his designee.

J. **Audit Trail:** All records of queries and responses in an ALPR system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the (1) date and time of access; (2) license plate number or other data elements used to query the system; (3) specific purpose, as set forth is subsection D, for accessing and querying the system, including the offense type for any criminal investigation; (4) associated case number or call for service number (CFS/CAD); and (5) username or the person(s) who accessed or queried the system.

K. **Query:** A search of ALPR system data based on information entered by the user, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the automatic license plate recognition system.

Operations

A. An ALPR system shall be accessed and used for official law enforcement purposes only and in compliance with § 2.2-5517, *Code of Virginia.* A user shall not use the 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 individuals.

1. A Query of the system shall contain an **Offense Type** and an **Incident (Case) Number or Call for Service Number**.
2. If a Query is run for another LE Agency (Virginia), the user must specify the Agency Name and include an Agency Case Number or Call for Service Number. If the requesting Agency is Out of State, legal process is required to comply with the request.

B. § 2.2-5517, section D, *Code of Virginia,* provides that a law-enforcement agency may use an ALPR system only (1) as part of a criminal investigation into an alleged violation of the Code of Virginia 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. A user shall not query or download system data unless such data is related to at least one of these purposes.

C. All information necessary for the creation of an audit trail shall be entered in order to query system data. The ALPR Program Manager or designated user may download audit trail data for the purpose of generating audit reports.

D. A stop of a motor vehicle based on a notification from the system shall be consistent with § 2.2-5517, section M, *Code of Virginia.*

E. Non-agency owned or contracted ALPR systems:

1. Users who have access to non-agency owned or contracted ALPR systems shall report such access to the ALPR Program Manager and/or other designee.

F. Notification of an Alert:

1. Notification by an ALPR system does not constitute reasonable suspicion as grounds for a deputy to stop a vehicle. Prior to stopping a vehicle based on a notification, a deputy shall:

   a. Verify the license plate number and state of origin to ensure that the alert is accurate;

   b. Confirm the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification (e.g., VCIN/NCIC); and

   c. Develop independent reasonable suspicion or probable cause before conducting stops, making detentions, or initiating arrests. Enforcement actions should **NOT** be taken solely based on an ALPR alert.

2. If a deputy stops the driver of a motor vehicle, stops and frisks a person based on reasonable suspicion, or temporarily detains a person during any other investigatory stop based upon the

alert of an ALPR, the reporting requirements set forth in § 52-30.2, section C, *Code of Virginia,* shall be followed (e.g., Community Policing Form).

ALPR Hot Lists

A. 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 local, state, or federal law enforcement agencies. Hot lists alert the user when such a vehicle is read by an ALPR camera in real time or by using historical ALPR data.

B. User generated hot lists shall be updated as soon as practical. ALPR systems utilizing the NCIC's Hot List will download the file at least once every 24 hours.

   1. Manually entered license plate lists shall contain at a minimum:

      a. Legal reasons for entry, including supporting information regarding why a particular license plate is on a specific hot list (e.g., stolen vehicle, suspect vehicle, missing/endangered person, etc.).

      b. Vehicle description, if available (e.g., year, make, model, and color).

      c. Valid 24-hour contact number of entrant or agency.

      d. A case number or CAD/CFS number.

Training Requirements

A. Employees must attend training prior to accessing or using the ALPR system.

   1. ALPR training will occur bi-annually and will include the following:

      a. Legal update of relevant ALPR matters

      b. Administrative procedures

      c. Technical procedures

   2. Agencies shall maintain a record of each employee's completion of ALPR training in accordance with existing training records policies.

System Data Usage, Retention, and Sharing

A. System data and audit trail data shall be purged as defined in § 2.2-5517, section E, *Code of Virginia.* This section mandates that ALPR system data shall be destroyed and not recoverable after 21 days of the date of its capture, and audit trail data shall be destroyed and not recoverable after two years of the date of its capture **UNLESS** the system data or audit trail data are part of an ongoing investigation, prosecution, or civil action.

1. Such data shall be retained by the Sheriff's Office until:

    a. The investigation concludes without any criminal charges; or

    b. 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.

B. System data dissemination, sharing, and disclosure are defined in § 2.2-5517, section F, *Code of Virginia.*

1. System data and audit trail data are **NOT** subject to disclosure under the Virginia Freedom of Information Act (FOIA).

2. ALPR system data may **NOT** be sold by its employees or its contracted ALPR vendor(s).

3. The Sheriff's Office shall not share system data or audit trail data with, or disseminate such data to, any database of any other state, federal, private, or commercial entity.

4. The Sheriff's Office may share system data or audit trail data for the following purposes:

    a. With another law-enforcement agency for the purposes set forth in subsection D, which may include allowing another law-enforcement agency to query system data, provided that the agency receiving such data shall comply with all the provisions of this section;

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

    b. With the attorney for the Commonwealth for the purposes set forth in subsection D, or for complying with discovery, or a court order in a criminal proceeding;

    c. With a defendant or his counsel for purposes of complying with discovery or a court order in a criminal proceeding;

    d. Pursuant to court order or a court-issued subpoena duces tecum in any criminal or civil proceeding;

    e. With the vendor for maintenance or quality assurance purposes; or

f. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding warrant.

ADMINISTRATIVE PROCESS

A. Internal system auditing shall occur at least once every 30 days by the ALPR Program Manager and/or designee.

1. Internal system audits shall be conducted in the following areas:

a. **Queries Conducted** - At least 5% of the total number of times the system was queried, including the specific purposes of the queries, as set forth in § 2.2-5517, section D, *Code of Virginia*, and the offense types for any criminal investigation.

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

c. **Traffic Stops** - At least 5% of the total monthly traffic stops conducted as the result of an ALPR alert to ensure compliance with § 2.2-5517, section M, *Code of Virginia* along with the reporting requirements set forth in § 52-30.2, section C, *Code of Virginia.*

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

2. ALPR data and audit trail data shall be purged and rendered not recoverable in accordance with § 2.2-5517, section E, *Code of Virginia.*

B. Data Security and Access

1. ALPR data is categorized as "Official Use Only" and is considered confidential in nature. Access control to the administrative profile(s) of the ALPR system shall be maintained.

2. Users will receive individualized logins to Flock's web-based server and shall not share their login information, including passwords, with others.

3. Access to ALPR data constitutes the user's consent to monitoring all logins and queries, and consent to the suspension and termination of their access privileges during and following an audit or investigation.

4. All collected data will not be connected to, or shared with, other law-enforcement databases.

5. Flock is Criminal Justice Information Services (CJIS) compliant, and all information is encrypted and is stored in the cloud using Amazon Web Services (AWS) Key Management Service (KMS) keys, which use Federal Information Processing Standard (FIPS) 140-2 validated hardware security modules to generate and store keys.

6. Unauthorized use, which includes requests, dissemination, sharing, copying, or receipt of ALPR data accessed through the Flock system could result in civil proceedings and/or criminal proceedings against any user and/or other person involved.

C. ALPR Program Manager

1. The Investigations Lieutenant and/or other designee who possesses decision making authority to manage the ALPR program.

2. The ALPR Program Manager and/or designee should at a minimum:

   a. Stay abreast of current case law and legislation;

   b. Monitor the use of the ALPR system and conduct monthly audits;

   c. Manage user accounts and permissions;

   d. Manage ALPR training;

   e. Update ALPR policy as necessary; and

   f. Shall file an ALPR report by April 1 each year on the previous calendar year's use of the system to the Virginia State Police as defined in § 2.2-5517, section I, *Code of Virginia*