

---

## Automated License Plate Readers (ALPRs)

### 430.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 430.2 DEFINITIONS

Definitions related to this policy include:

**Automated License Plate Reader (ALPR):** A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

**ALPR Operator:** Trained Office members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Office, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts

**ALPR Administrator:** The Special Services Captain or the Sheriff's designee, serves as the ALPR Administrator for the Office.

**Hot List:** A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA DMV, Local BOLO's, etc.

**Vehicles of Interest:** Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.

**Detection:** Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

**Hit:** Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

### 430.3 POLICY

The policy of the Sonoma County Sheriff's Office is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

See attachment: [NCRIC\\_ALPR\\_PrivacyPolicy.pdf](#)

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

#### **430.4 ADMINISTRATION**

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Sonoma County Sheriff's Office to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Special Services Captain. The Special Services Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

##### **430.4.1 ALPR ADMINISTRATOR**

The Special Services Captain shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53)

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Working with the Custodian of Records on the retention and destruction of ALPR data.
- (g) Ensuring this policy and related procedures are conspicuously posted on the department's website.

#### **430.5 DATA COLLECTION AND RETENTION**

The Special Services Captain responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

#### **430.6 ALPR DATA FROM PARKING ENFORCEMENT OPERATIONS**

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

#### **430.7 ALPR DATA FROM FIXED CAMERA SYSTEM(S)**

ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil 430.4.3action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

ALPR vendor will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. ALPR vendor will purge their data at the end of the 30 days of storage. However, this will not preclude Sonoma County Sheriff's Office from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established County of Sonoma retention schedule mentioned above or outlined elsewhere.

#### **430.8 RESTRICTIONS ON THE USE OF ALPR DATA**

Information gathered or collected, and records retained by ALPR vendor(s) will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

#### **430.9 OPERATIONS**

Use of an ALPR is restricted to the purposes outlined below. Office members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

1. An ALPR shall only be used for official law enforcement business.
2. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
3. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
4. No member of this office shall operate ALPR equipment or access ALPR data without first completing office-approved training.
5. No ALPR operator may access office, state or federal data unless otherwise authorized to do so.
6. If practicable, the deputy should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator should confirm that the observed license plate from the system matches the license plate

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a CLETS inquiry via MDC or through Dispatch. Members will not take any enforcement action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, deputies are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Deputies should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

7. Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Office's LPR system may be updated by agency sources more frequently than the Office may be uploading them and thus the Office's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Office members shall undertake the following:
  - (a) Verification of status on a Hot List. A deputy must receive confirmation, from a Sonoma County Sheriff's Office Communications Dispatcher or other office computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
  - (b) Visual verification of license plate number. Deputies shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the LPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Office members alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a office member would have a lawful basis to stop the vehicle.
  - (c) Office members will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation of the ALPR Hit and the arrest, then the Office member shall update with the Communications Dispatcher and original person and/or a crime analyst inputting the vehicle in the hot list (hit).
  - (d) General Hot Lists (SVS, SFR, and SLR) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.
  - (e) All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Office member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system.

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Office member's immediate supervisor. The hits from these data sources should be viewed as informational; created solely to bring the deputies attention to specific vehicles that have been associated with criminal activity.

8. All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:
  - (a) Entering Office member's name
  - (b) Short synopsis describing the nature of the originating call
  - (c) Related case number.
9. Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.
10. Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Sonoma County Sheriff's Office. Office personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:
  - (a) Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
  - (b) Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
  - (c) Use Based on a Protected Characteristic. It is a violation of this policy to use the LPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
  - (d) Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
  - (e) First Amendment Rights. It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.
  - (f) Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to
    - (a) Criminal prosecution
    - (b) Civil liability, and/or

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

- (c) Administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Office policies

#### **430.10 ACCOUNTABILITY**

All data will be closely safeguarded and protected by both procedural and technological means.

The Sonoma County Sheriff's Office will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- (c) ALPR system audits should be conducted on a regular basis. For security or data breaches, see the Records Release and Maintenance Policy.

#### **430.11 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  1. The name of the agency.
  2. The name of the person requesting.
  3. The intended purpose of obtaining the information.
- (b) The request is reviewed by the Special Services Captain or the authorized designee and approved before the request is fulfilled.
- (c) The Sheriff or the authorized designee will consider the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the release of ALPR data. The Sonoma County Sheriff's Office does not permit the sharing of ALPR data gathered by the County, or contract Cities or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

# Sonoma County Sheriff's Office

## Policies

### *Automated License Plate Readers (ALPRs)*

---

- (d) ALPR data will not be shared or released to any agency outside of the State of California, absent a court order from a Magistrate from the State of California.
- (e) The approved request is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).
- (f)

## **Attachments**



## **NCRIC\_ALPR\_PrivacyPolicy.pdf**

## NCRIC MISSION

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens of the fifteen Bay Area counties within its area of responsibility from the threat of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

## AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGIES

To support authorized law enforcement and public safety purposes of local, state, federal, and tribal public safety agencies, the NCRIC utilizes Automated License Plate Reader (ALPR) technology, and supporting software, to gather and analyze ALPR data to enable the rapid identification and location of vehicles of legitimate interest to law enforcement. ALPR units are attached to law enforcement vehicles or deployed at fixed locations, where they collect license plate information from vehicles on public roadways and public property. In one common use of ALPR technology, license plate encounters are compared against law enforcement "hotlists", lists of vehicles associated with active investigations, for example, related to Amber Alerts or other missing children, stolen vehicles, or stolen license plates. The information is also retained for a fixed retention period, though it is only re-accessible by law enforcement given a legitimate law enforcement purpose as listed below.

## PURPOSE

This NCRIC Automated License Plate Reader Policy (ALPR Policy) defines a minimum set of binding guidelines to govern the use of Automated License Plate Reader Data (ALPR Data), in order to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties.

The NCRIC also completed a NCRIC ALPR Privacy Impact Assessment (PIA) to address in further detail common privacy and civil liberties concerns regarding Automated License Plate Reader technology. The current version of this document is available on the NCRIC web site at [www.ncric.org](http://www.ncric.org).

## AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA

To support the mission of the NCRIC, Law enforcement personnel with a need and right to know will utilize ALPR technology to:

- Locate stolen, wanted, and subject of investigation vehicles;

- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;

- Locate witnesses and victims of violent crime;

- Locate missing children and elderly individuals, including responding to Amber and Silver Alerts;

- Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;

- Protect participants at special events; and
- Protect critical infrastructure sites.

#### RESTRICTIONS ON COLLECTION OF ALPR DATA AND USE OF ALPR SYSTEMS

NCRIC ALPR units may be used to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

ALPR operators must recognize that the data collected from the ALPR device, and the content of referenced hotlists, consists of data that may or may not be accurate, despite ongoing efforts to maximize the currency and accuracy of such data. To the greatest extent possible, vehicle and subject information will be verified from separate Law enforcement information sources to confirm the vehicle or subject's identity and justification for contact. Users of ALPR Data must, to the fullest extent possible, visually confirm the plate characters generated by the ALPR readers correspond with the digital image of the license plate in question.

All users of NCRIC ALPR equipment or accessing NCRIC ALPR Data are required to acknowledge that they have read and understood the NCRIC ALPR Policy prior to use of the ALPR System.

In no case shall the NCRIC ALPR system be used for any purpose other than a legitimate law enforcement or public safety purpose.

#### TRAINING

Only persons trained in the use of the NCRIC ALPR system, including its privacy and civil liberties protections, shall be allowed access to NCRIC ALPR Data. Training shall consist of: •Legal authorities, developments, and issues involving the use of ALPR Data and technology

- Current NCRIC Policy regarding appropriate use of NCRIC ALPR systems;
- Evolution of ALPR and related technologies, including new capabilities and associated risks;
- Technical, physical, administrative, and procedural measures to protect the security of ALPR Data against unauthorized access or use; and
- Practical exercises in the use of the NCRIC ALPR system

Training shall be updated as technological, legal, and other changes that affect the use of the NCRIC ALPR system occur. In no case shall a person utilize the NCRIC ALPR system if he/she has not completed training in more than a year.

#### AUDIT

Access to, and use of, ALPR Data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- The name of the law enforcement user;
- The name of the agency employing the user;
- The date and time of access;
- The specific data accessed;
- The supplied authorized law enforcement or public safety justification for access; and
- A case number associated with the investigative effort generating the ALPR data query.

Audit reports will be provided periodically and on request to supervisory personnel at the NCRIC and partner agencies.

In addition, no less frequently than every 12 months, the NCRIC will audit a sampling of ALPR system utilization from the prior 12 month period to verify proper use in accordance with the above authorized uses. Any discovered intentional misconduct will lead to further investigation, termination of system access, and notification of the user's parent agency for appropriate recourse. In addition, the auditing data will be used to identify systemic issues, inadvertent misuse, and requirements for policy changes, training enhancements, or additional oversight mechanisms.

These ALPR audits shall be conducted by a senior NCRIC official other than the person assigned to manage the NCRIC ALPR function. Audit results shall then be reported to the Director of the NCRIC.

#### DATA QUALITY AND ACCURACY

The NCRIC will take reasonable measures to ensure the accuracy of ALPR Data collected by NCRIC ALPR units and partner agency ALPR systems. Errors discovered in ALPR Data collected by NCRIC ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question. Errors discovered in ALPR Data collected from partner agencies' ALPR systems are communicated back to the controlling agency to be addressed as deemed appropriate by that agency or in accordance with the agency's own ALPR data policies.

As the downstream custodian of "hotlists", the NCRIC will provide the most recent versions of these lists available and ensure the lists are refreshed from state or federal sources on a daily basis.

The NCRIC acknowledges that, in rare instances ALPR units may inadvertently capture information contrary to the collection guidelines set forth in this policy. Such records will be purged upon identification. Any discovered notable increase in frequency of these incidents from specific ALPR units or agencies will be followed up with for equipment repairs, camera realignment, or personnel training as necessary.

#### PHYSICAL AND ELECTRONIC SECURITY OF ALPR DATA:

Data collected by ALPR systems is stored in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff in good standing who have completed background investigations and possess an active security clearance at the "SECRET" or higher level.

NCRIC will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

#### RETENTION OF ALPR DATA:

ALPR records matching an entry in a current law enforcement hotlist will trigger an immediate notification to the officer operating the ALPR unit, the active dispatch officer at the agency owning the ALPR unit, the NCRIC, and the custodial agency of the hotlist. Such notifications are also subject to a maximum retention of 12 months.

ALPR Data obtained with license plate information not appearing on hotlists, and with no immediate reasonable connection to criminal activity, will be retained in secure systems so as to only be made accessible to authorized personnel for a maximum period of twelve months, then purged entirely from all systems. If during the specified retention period there is information which supports a legitimate law enforcement purpose (see above section enumerating AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA) as to a license plate or partial license plate which was recorded and is retained in these systems, then limited access will be permitted for predicate-based querying for potential matches against the parameters specific to the legitimate law enforcement purpose. Such events shall be recorded in an access log showing date, time, name of person seeking access, agency of employment, reason for access, and tracking identifiers such as an agency case number.

ALPR records of vehicles having been identified and linked to criminal investigation will be entered into the relevant NCRIC database(s) and retained for a period of no more than five years. If during the five-year period NCRIC personnel become aware that the vehicle license plate information is no longer associated with a criminal investigation, it will be purged from the NCRIC's databases.

#### CUSTODIAN OF RECORDS AND RECORDS REQUESTS

Each agency sharing data retains control and ownership as the official custodian of its records, and must independently verify all external information obtained via NCRIC Information Systems. To the extent permitted by law, requests for information under the California Public Records Act or Freedom of Information Act or similar applicable laws will be directed back to the owner of the requested data.

#### SYSTEM MANAGEMENT AND ACCOUNTABILITY

The NCRIC shall assign a senior officer who will have responsibility, and be accountable, for managing the ALPR Data collected and ensuring that the privacy and civil liberties protection and other provisions of this ALPR Policy are carried out. This individual shall also be responsible for managing a process for maintaining the most current and accurate hotlists available from NCRIC law enforcement sources. This individual shall also have the responsibility for the security of the hotlist information and any ALPR Data which is maintained by the NCRIC. It remains, however, the personal responsibility of all officers with access to ALPR Data to take reasonable measures to protect the privacy and civil liberties of individuals, as well as the security and confidentiality of ALPR Data.

#### COMMERCIALY CREATED ALPR DATA

Except as explicitly authorized below with regard to critical infrastructure, the NCRIC will not share NCRIC or partner agency ALPR Data with commercial or other private entities or individuals.

#### DISSEMINATION

The NCRIC may disseminate ALPR data to any governmental entity with an authorized law enforcement or public safety purpose for access to such data. The NCRIC assumes no responsibility or liability for the acts or omissions of other agencies in making use of the ALPR data properly disseminated. Though the NCRIC will make every reasonable effort to ensure the quality of shared ALPR Data and hotlists, it cannot make absolute guarantees of the accuracy of information provided.

ALPR Information may be disseminated to owners and operators of critical infrastructure in circumstances where such infrastructure is reasonably believed to be the target of surveillance for the purpose of a terrorist attack or other criminal activity. In these situations, the NCRIC also will make notification to appropriate local, state, and federal law enforcement agencies.

Information collected by the ALPR system shall not be disseminated to private parties, other than critical infrastructure owners or operators, as limited above, unless authorized, in writing, by the Director of the NCRIC or his designee. ALPR information shall not be disseminated for personal gain or for any other non-law enforcement purposes.

#### POLICY REVISIONS

NCRIC ALPR Policies will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations.