

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

463.1 PURPOSE AND SCOPE

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

ALPR technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Orange County Sheriff-Coroner Department to link data associated with vehicle license plates for official law enforcement purposes, including identifying and locating stolen or wanted vehicles, stolen license plates and missing persons. ALPRs may also be used to gather or disseminate information related to active warrants, homeland security advisories (as permitted by California law), law enforcement bulletins, electronic surveillance, suspect interdiction, and stolen property recovery. It is the intent of the Department to ensure that the access and use of ALPR data is consistent with the law and with respect for individuals' privacy and civil liberties. The Department will also investigate and enforce unauthorized disclosure of confidential information. See Policy 215 and Civil Code 1792.29.

463.2 ADMINISTRATION

All installation and maintenance of department owned/leased ALPR equipment shall be managed by the Technology Division. The acquisition of ALPR systems and data shall be the responsibility of the Technology Division. The Technology Division will be responsible for ensuring vendors have the required safeguards that comply with CJIS standards. Data collected by Department owned/leased ALPR equipment, unless copied and booked as evidence, shall be managed by the ALPR provider. The Technology Division shall oversee the access, sharing, and technical requirements of this policy. The Patrol Operations Command shall oversee compliance, training, audit and use requirements of this policy. The administration of this policy shall be in compliance with the requirements of Civil Code Section 1798.90.5 et seq.

463.3 OPERATIONS

Use of an ALPR is restricted to the purposes outlined in this policy. Only Department Members assigned as Sergeants, Deputy Sheriffs, Investigators, Investigative Assistants, Dispatchers, Analysts, Sheriff Special Officers (SSO) or Community Service Officers (CSO) AND assigned to the Patrol Operations Command, Investigations and Special Operations Command, Judicial Protection Unit, Orange County Intelligence Assessment Center (OCIAC), Internal Affairs Bureau, or Regional Narcotics Suppression Program (RNSP) are authorized to operate ALPR equipment and access ALPR data, provided they have first received Department approved training. Department 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.

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

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, arson events, bombings, 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 Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.
5. No ALPR operator may access Department, state, or federal data unless otherwise authorized to do so.
6. The user shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.
7. Department Members shall access ALPR only from an approved Department workstation, MDC, or Department-issued mobile device.
8. Deputies are not authorized to respond Code 3 to an ALPR "hit" unless exigent circumstances exist and must comply with OCSD Policy 316.
9. No member of this Department is authorized to leave a call for service in response to an ALPR "hit" unless there is an exigent circumstance.
10. Non-criminal history information contained within databases accessed through CLETS, NCIC or other DOJ criminal justice systems, as well as California LEAs' individual databases should not be used for the purpose of immigration enforcement.
11. Users should not include criminal history information or other personal identifying information of a target suspect (beyond the suspect's last name) or information obtained from CLETS into ALPR information fields accessed by those not authorized to receive CLETS information.

463.4 DATA COLLECTION AND RETENTION

All ALPR data is hosted or otherwise provided using a "Third Party ALPR Provider" (such as those contracts originated by the Department, law enforcement contract partners, businesses, homeowners' associations ("HOAs", etc.). ALPR data that is provided by the Third Party ALPR provider is the sole responsibility of that company (service provider). The Third Party ALPR Provider owns and is solely responsible for the data it makes available, its data will not be stored outside of the United States or Canada, and its employees who have access to unencrypted criminal justice information will undergo training and background checks.

ALPR data collected by the Department will be retained for six months to allow for the proper investigation into reported criminal activity. All data captured after six months will be purged unless it is part of an active criminal investigation or booked as evidence.

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

ALPR data used in a criminal investigation may be considered evidence and should be exported, submitted into evidence, and documented in the related case report. All ALPR data uploaded to the Department's Digital Evidence Management System (DEMS) or copied and booked as evidence, shall follow the Department's evidence booking, handling, storage, and retention requirements.

463.5 ACCOUNTABILITY

All data shall be closely safeguarded and protected by both procedural and technological means. Each Member is responsible for safeguarding their personal login and password. The Orange County Sheriff-Coroner Department shall observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, time, and purpose (Case #) (Civil Code § 1798.90.52). If applicable, multi-factor or two-factor authentication will be utilized in addition to login/password.
2. 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 relates to a specific criminal investigation or Department-related civil or administrative action. A report number or CAD call number shall be inputted into the search justification field before searching the ALPR data.
3. Members approved to access ALPR data will receive relevant training prior to independently accessing the data.
4. Any time an authorized Member reasonably believes ALPR data may be beneficial in a criminal or non-criminal matter, the Member shall input a detailed reason for access, report number or CAD call number into the search reason field, to access the ALPR database.
5. ALPR system audits shall be conducted on a regular basis to ensure the security of the information accessed or used is in compliance with all applicable privacy laws. The Technology Division will generate an ALPR use report. The report will be used to conduct monthly audits of ALPR responses. The audits will be conducted by the supervisor responsible for administrative duties where the ALPR user is assigned. Any potential violation of the law or Department policy will be forwarded to the Command of the involved member for further investigation which may result in revocation of ALPR system access, training and/or discipline.
6. Members of the Technology Division will be the only members to have and grant administrator access. Upon separation from the Department, access to any ALPR data will be immediately revoked.
7. The Technology Division Director or designee will be the official custodian of the ALPR systems. The Technology Division will provide a list of users during the Employee Life Cycle review. The list will be given to the divisions to conduct a user audit by the supervisor responsible for administrative duties where the ALPR user is assigned.

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

8. Members using ALPR must recognize that the data collected from the ALPR device, and the content of the referenced Hot Lists, consists of data that may or may not be accurate. To the greatest extent possible, information obtained from ALPRs should 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 license plate or vehicle characteristics correspond with the digital image of the license plate or vehicle generated by the ALPR.
9. Members using ALPR will be required to implement the reasonable security features outlined in this policy pursuant to Cal. Civil Code 1798.90.51.
10. All Members using ALPR equipment or accessing ALPR data are required to acknowledge that they have read and understood this policy prior to use of the ALPR System.

463.6 AUDITS

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

1. The name of the user;
2. The date and time of access;
3. The specific data accessed;
4. The supplied authorized law enforcement or public safety justification for access; and
5. A case, tip, or CAD call number associated with the investigative effort generating the ALPR data query.

463.7 THIRD PARTY ALPR

Many local governments, businesses and HOAs have entered contracts with companies who provide ALPR services ("Third Party ALPR" providers). The Orange County Sheriff's Department can use ALPR equipment and data owned by Third Party ALPR providers if there is an agreement with the contracting entity. Allied law enforcement agencies can also share their ALPR data with members from the Orange County Sheriff's Department. Third Party ALPR data is to be handled consistent with California Civil Code sections 1798.90.5 et seq.

The owner of the "Third Party ALPR" system is responsible for the retention of data, as well as, any PRA requests related to the system they own. Any PRA requests for data from a Third Party ALPR system shall be governed by the Third Party ALPR provider's PRA policy and practices. Members of the Orange County Sheriff's Department will not retain data from "Third Party ALPR" systems unless that specific information is used during official OCSD duties and saved by OCSD.

463.8 CREATION AND USE OF "HOT LIST" OR "CUSTOM HOT LISTS"

Hot Lists are lists of vehicles or license plates associated with active investigations. Third party ALPR systems may automatically generate Hot Lists for license plate information that has been

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

entered into the California Law Enforcement Telecommunication System (CLETS). Examples of investigations include Amber Alerts or other missing children, Silver Alerts or other critical missing elderly persons, missing adults, stolen vehicles, or stolen license plates. The purpose of these lists is to alert OCSD personnel that a vehicle displaying a license plate number that is included on a Hot List has been observed by an ALPR camera.

Custom Hot Lists can also be created for active investigations or official department business but may only be created by authorized members.

1. Authorized members permitted to create a "Custom Hot List" include:
 - (a) Deputies assigned to the Real Time Operations Center (RTOC)
 - (b) Investigators
 - (c) Investigative Assistants
 - (d) Research/Crime Analysts
 - (e) Sergeants
 - (f) Deputy IIs assigned to the Traffic Office responsible for Traffic Collision Investigations
2. All Custom Hot Lists must be approved by a Sergeant prior to posting or distributing.
3. When a member receives a Hot List or Custom Hot List alert, the member must verify:
 - (a) The ALPR read was accurate.
 - (b) The issuing state matches the plate on record.
 - (c) The circumstances that triggered the alert for a stolen vehicle or lost/missing/stolen license plate are still valid by verifying through CLETS.
 - (d) Circumstances that triggered the alert for all other cases not listed in subsection (c) must be accompanied with independent reasonable suspicion or legal justification for a detention.
 - (e) The type of response requested in a Custom Hot List entry (e.g., Stop and FI, Crime Vehicle, Felony Warrant, etc.).
4. If the record in the Hot List or Custom Hot List was created based on the wanted status of the registered owner (the registered owner has an outstanding warrant for their arrest), the Department Member must be cognizant of the fact the driver may not be the wanted subject and should have independent reasonable suspicion or legal justification for the stop.
5. Members must have reasonable suspicion to initiate a traffic enforcement stop on the vehicle, independent from the Hot List or Custom Hot List alert.

463.9 SHARING AND RELEASING ALPR DATA

Pursuant to Civil Code Section 1798.90.55, subdivision (b), ALPR data shall not be sold, shared, or transferred, except to another public agency, and only as otherwise permitted by law. SB 34 does not permit California LEAs to share ALPR information with private entities or out-of-state

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

or federal agencies, including out-of-state and federal law enforcement agencies. Members may share ALPR data on a case-by-case basis with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the ALPR data that includes:
 - (a) The name and description of the agency.
 - (b) The name of the person requesting the information.
 - (c) The intended purpose of obtaining the information.
 - (d) A statement that the data will be kept confidential and will not be used or disclosed in any manner that is prohibited by California Civil Code section 1798.90.5 et seq.; Penal Code section 13778.2; Government Code sections 7284.6 and 7921.505, subdivision (c)(5); or any other laws that currently exist.
2. The request must be reviewed by the authorized designee within the Records Division and approved before the request is fulfilled.
3. The approved request is sent to the Technology Division and is retained on file by the Technology Division according to the County of Orange retention requirements.

ALPR data authorized to be shared with other Law Enforcement agencies for access to the requesting agency's independent ALPR searches must be accompanied by the Department's ALPR Sharing MOU. The Technology Division will retain all ALPR MOUs, grant/deny access to the requesting agency, and ensure compliance with MOU requirements.

Requests for ALPR data by non-law enforcement or non-prosecutorial public agencies shall be processed at the direction of the Records Division. (See Section 463.7 Third Party ALPR above regarding PRA requests involving Third Party Providers.)

In responding to a Public Records Act request or compulsory process in litigation seeking the production of ALPR information, California LEAs should consider all applicable privileges and exemptions depending on the nature of the request, bearing in mind the command in Civil Code section 1798.90.55, subdivision (b), that an ALPR end-user or operator "shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law."

The release of ALPR data which has been uploaded to the DEMS or copied to disc format and booked into evidence shall be released in accordance with Policy 802 - Property and Evidence.

463.10 TRAINING

Department training for use of ALPR systems shall address compliance with this policy including data privacy and security.

The Field Training Bureau shall ensure that members assigned to the Patrol Operations Command receive Department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Automated License Plate Readers (ALPRs) Usage and Privacy Policy

The Real Time Operations Center Supervisor will ensure that Members assigned to the Operations Support & Intelligence Division, and any other authorized user receive Department-approved training for those authorized to use or access the ALPR system through OCSD access (Civil Code § 1798.90.51; Civil Code § 1798.90.53).