

Automated License Plate Readers (ALPRs)

430.1 PURPOSE AND SCOPE

ALPR technology is a computer-based system that utilizes special cameras to capture license plate information. The ALPR system captures an infrared license plate image and converts it to a text file using Optical Character Recognition ("OCR") technology. The text is compared to various hotlists generated by local, state, and federal law enforcement agencies, including the National Crime Information Center ("NCIC"), and generates an alert when there is a hit. The ALPR system identifies license plates and will not identify the person operating the motor vehicle. The Department may, as a separate step and for legitimate law enforcement purposes per the Federal Driver's Privacy Protection Act, and as set forth in this Policy, undertake to identify the owner of a vehicle in the event the ALPR system generates an alert such as by running the license plate number through the State of California Department of Motor Vehicle (DMV) database.

The ALPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals include but are not limited to, providing information to officers that will assist in ongoing criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in our community through the identification and removal of stolen or unregistered motor vehicles.

The Department shall utilize hot lists which further the above specified goals of the ALPR system, where there is a legitimate and specific law enforcement reason for identifying a vehicle associated with an outstanding arrest warrant, vehicles related to missing persons investigations, vehicles associated with AMBER Alerts, stolen vehicles, vehicles that are reasonably believed to be involved in the commission of a crime, vehicles which are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list, vehicles with expired registrations, vehicles registered to persons who are subject to a restraining order issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements, vehicles registered to persons wanted by a law enforcement agency who are of interest in a specific investigation, or vehicles registered to persons who are on any watch list issued by a State or Federal agency responsible for homeland security when information has been received concerning a specific individual.

430.2 POLICY

The policy of the Palm Springs Police Department 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.

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

It shall be the policy of the Palm Springs Police Department that all Department members abide by the policy and its procedures set forth when using the ALPR system, thereby increasing the efficiency and effectiveness of its public safety efforts in a manner that safeguards the privacy concerns of law abiding citizens.

430.3 DEFINITIONS

- (a) **Automated License Plate Reader (ALPR):** A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest.
- (b) **Automated License Plate Reader (ALPR) System:** The computerized storage system of data collected from Automated License Plate Readers.
- (c) **Hit Alert:** An audible and/or visual signal from the ALPR System activated upon the read of a license plate by the ALPR System that has NOT BEEN VISUALLY VERIFIED by the ALPR operator against the photo in the ALPR System. A Hit Alert from the ALPR system may indicate that a scanned license plate number may be in the NCIC or other law enforcement database for a specific reason, including, but not limited to, being related to a stolen car, wanted person, wanted vehicle, missing person, domestic violence protective order or terrorist-related activity.
- (d) **Hot List:** A list of license plates associated with vehicles of interest from databases including, but not limited to National Crime Information Center (NCIC), Department of Motor Vehicles (DMV), and vehicles sought by local law enforcement agencies.
- (e) **Detection:** Data obtained by an ALPR of license plates within public view that were read by an ALPR device, including potential images of the license plate and vehicle on which it was displayed, and information regarding the location of the ALPR equipment at the time of the detection.

430.4 ALPR ADMINISTRATOR

The Police Captain overseeing the Operations Division 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.

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

- (g) Ensuring this policy and related procedures are conspicuously posted on the Police Department website.
- (h) Shall submit a quarterly ALPR System Audit Report and Total Detection Report to the Chief of Police.
- (i) All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the ALPR Administrator who will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

430.4 AUTHORIZED USERS

The ALPR System shall only be accessed by the following Police Department positions after the completion of Department approved training and upon the approval of the ALPR Administrator:

- (a) Police Officers
- (b) Police Sergeants
- (c) Police Lieutenants
- (d) Police Captains
- (e) Police Chief
- (f) Police Dispatchers
- (g) Crime Analyst
- (h) Community Service Officers
- (i) City approved contractor for ALPR system maintenance.

430.6 ALPR OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. 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).

- (a) An ALPR shall only be used for official law enforcement business.
- (b) 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.
- (c) 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.
- (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training and receiving ALPR Administrator approval.

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

- (e) No ALPR operator may access department, state or federal data unless otherwise authorized to do so.
- (f) ALPR operators shall ensure ALPR cameras are properly affixed to the assigned police vehicle prior to starting their shift and shall inspect the equipment for damage or excessive wear.
- (g) ALPR operators shall ensure the ALPR system is functioning properly at the start of their shift.
- (h) ALPR operators shall report any damage, excessive wear, and/or function issues to the ALPR Administrator via Department email immediately.
- (i) Login/Log-Out Procedure- To ensure proper operation and to security oversight of the ALPR system, all operators will be required to have individual credentials for access and use of the systems and/or data.
- (j) Any potential data breaches of the ALPR system shall be reported to the ALPR Administrator immediately.
- (k) When an ALPR Detection alarm is received alerting an ALPR Operator of a positive Hit from the ALPR database, operators shall compare the digital image of the license plate to the Hotlist information to verify the Hit for both the state and characters on the license plate. Absent exigent circumstances, ALPR Operators shall confirm the ALPR information via radio or mobile data computer to immediately confirm the Hit prior to taking enforcement or any other type of police action
- (l) If an alert is received on an incorrect letter or number on a license plate, the user should correct the number received on the hit for accurate information if the correct information is available.

430.7 ALPR SYSTEM OPERATIONS

Use of the ALPR System is restricted to the purposes outlined below. Department members shall not use the system for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) The ALPR system shall only be used for official law enforcement purposes.
- (b) No member of this department shall be permitted to access the ALPR System without first completing department-approved training and receiving ALPR Administrator approval.
- (c) Database information shall be considered confidential and for law enforcement personnel only.
- (d) Login/Log-Out Procedure- To ensure proper operation and to security oversight of the ALPR system, all operators will be required to have individual credentials for access and use of the systems and/or data.
- (e) ALPR System Users shall not allow non-authorized users to view system data.
- (f) Access to the ALPR system shall be from Department issued or Department owned computer equipment and shall not be accessed from personally owned devices without written permission from the ALPR Administrator.

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

- (g) All queries of system data shall include the reason for query and any applicable event number associated with query.
- (h) Any potential data breaches of the ALPR System shall be reported to the ALPR Administrator immediately.
- (i) The Palm Springs Police Department shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.

430.8 DATA COLLECTION AND RETENTION

The Operations Division Captain is responsible for ensuring that systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles or fixed locations to the designated storage in accordance with department procedure.

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

All ALPR data downloaded should be stored for no longer than one year, and in accordance with the established records and retention protocols. 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 to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence until the pending litigation is resolved (Government Code § 34090.6).

ALPR technology uses cameras to capture and store images from public spaces, where persons do not have a reasonable expectation of privacy. All videos gathered by these systems are for the official use of this department. The ALPR cameras will be positioned to optimize collection of images from public places to minimize collection of images from places where an expectation of privacy exists or places exposed to view (e.g., parking lot of a shop or business).

430.9 ACCOUNTABILITY AND PRIVACY

All personnel authorized to use or access ALPR System data will be accountable for knowledge of this policy. All personnel shall report errors and suspected or confirmed violations of this policy to their supervisor.

All access to the system will be logged and the Department will maintain an audit trail of requested and accessed information, including the purpose of the query.

All data will be closely safeguarded and protected by both procedural and technological means. The Palm Springs Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

- (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) Persons 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) The ALPR System database and software resides in a data center featuring full redundancy and access controls.
- (d) All investigative queries into collected ALPR data are logged by user and available for auditing and review by the Department as outlined in this policy.
- (e) ALPR system audits should be conducted on a regular basis. To ensure proper oversight into the use of the system and adherence to this policy, all activities (plate detections, queries, reports, etc.) are automatically recorded by the system for auditing purposes. System audits shall be conducted by the Operations Captain quarterly. The audit report shall include an explanation regarding any data retained longer than two years (e.g. data retained as evidence in a criminal case).
- (f) Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Department. Department 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, it 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) 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.
- (d) Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to:
 - criminal prosecution,
 - civil liability, and/or
 - administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

For security or data breaches, see the **Records Release and Maintenance Policy**.

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

430.10 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:
 - (a) The name of the agency.
 - (b) The name of the person requesting.
 - (c) The intended purpose of obtaining the information.
- (b) The request is reviewed by the Chief of Police or the authorized designee and approved before the request is fulfilled.
- (c) The approved request is retained on file.
- (d) Detection data will only be shared with law enforcement agencies who utilize the Law Enforcement Archival Reporting Network unless approved by the ALPR Administrator.
- (e) Detection data shall not be sold or transferred to non-law enforcement entities or persons.
- (f) Detection data will not be shared with federal immigration agencies or with law enforcement agencies outside of the State of California, absent a court order or special request submitted to PSPD explaining the intended purpose of obtaining the information, and only with approval from the Chief of Police, or their designee.

Memorandum of Understanding

- (a) Access to searchable data by other local law enforcement agencies shall only be granted pursuant to an MOU with that specific agency
- (b) Such MOU will provide that access will only be used for legitimate law enforcement or public safety purposes

The Chief of Police or the authorized designee will comply with the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the access to ALPR data. The Palm Springs Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.

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).

430.11 TRAINING

The Training Sergeant should ensure that members receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

Palm Springs Police Department

Policies

Automated License Plate Readers (ALPRs)

Each approved user shall have received CLETS Security Training and Approval, department approved ALPR training, and any required POST approved training prior to access or use of the ALPR System.

The training shall include user acknowledgement of this Policy.