


DEPARTMENT OF JUSTICE
DIVISION OF LAW ENFORCEMENT
GENERAL ORDER

SUBJECT: Automated License Plate Readers	ORDER NUMBER: 2023-05 DATE ISSUED: October 27, 2023
REFERENCE: Supersedes Law Enforcement Policy and Procedures Manual Section 429	APPROVED BY:  John D. Marsh, Chief

The Division of Law Enforcement (DLE) is currently updating the California Department of Justice (DOJ) Law Enforcement Policy & Procedures Manual. In the interim, this General Order shall serve as direction regarding Automated License Plate Readers.

429 Automated License Plate Readers

429.1 MISSION

This policy provides employees and the public with guidance regarding DOJ’s access, use, sharing, storage and retention of “automated license plate recognition” (ALPR) information. The DOJ, through its DLE and Division of Medi-Cal Fraud & Elder Abuse (DMFEA) (together, the “DOJ”), accesses ALPR information, defined below, in order to further its mission of ensuring the public safety of California residents. In doing so, DOJ is committed to complying with all applicable laws, including those laws related to the access, use, sharing, storage and retention of ALPR information.

429.2 DEFINITIONS

For purposes of this policy, the following definitions apply:

- **“ALPR information”** is “information or data collected through the use of an ALPR system.” (Civ. Code, § 1798.90.5, subd. (b).)
- **“ALPR system”** means “a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.” (Civ. Code, § 1798.90.5, subd. (d).)
- **“ALPR operator”** is “a person that operates an ALPR system,” with exclusions not relevant to the DOJ’s policy. (Civ. Code, § 1798.90.5, subd. (c).)
- An **“ALPR end-user”** is “a person that accesses or uses an ALPR system,” with exclusions

not relevant to the DOJ's policy.¹ (Civ. Code, § 1798.90.5, subd. (a).)

- A **“person”** is “any natural person, public agency, partnership, firm, association, corporation, limited liability company, or other legal entity.” (Civ. Code, § 1798.90.5, subd. (e).)
- A **“public agency”** is “the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency.” (Civ. Code, § 1798.90.5, subd. (f).)

429.3 AUTHORIZED PURPOSE

ALPR information assists DOJ in its enforcement of federal and California laws. ALPR information is collected through an ALPR system, which consists of fixed and mobile cameras that capture images of license plates within their field of view.

The DOJ does not own or operate any fixed or mobile cameras, nor does it maintain a searchable computer database that contains ALPR information. Rather, it utilizes ALPR information that is collected by other law enforcement agencies and commercial entities that operate ALPR systems. Because the DOJ does not maintain an ALPR system but rather only accesses ALPR information that is collected by other agencies or entities, it is considered an “end-user” of this information, and not an ALPR system operator.

429.4 ADMINISTRATOR AND PERSONS AUTHORIZED TO ACCESS ALPR INFORMATION

Access to ALPR information is limited to employees who need the data for an authorized purpose. The DOJ shall designate an “ALPR Administrator,” who shall be responsible for authorizing access to and use of ALPR information, and ensuring compliance with this policy and Civil Code 1798.90.5, *et seq.* For DLE, the ALPR Administrator shall have a minimum classification of Staff Services Analyst in the Office of the Chief. For DMFEA, the ALPR Administrator shall have the classification of Crime Analyst Supervisor (CAS).

The ALPR Administrators are responsible for authorizing the DOJ's access to ALPR systems and for authorizing specific DOJ employees to access such ALPR information. Only employees within a minimum classification of Special Agent or Crime Analyst shall be authorized to access ALPR information. DOJ employees shall only be given access for an authorized purpose, i.e., the

¹ Those exclusions are:

“(1) A transportation agency when subject to Section 31490 of the Streets and Highways Code.

(2) A person that is subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

(3) A person, other than a law enforcement agency, to whom information may be disclosed as a permissible use pursuant to Section 2721 of Title 18 of the United States Code.” (Civ. Code, § 1798.90.5, subd. (a).)

enforcement of federal and California laws.

The ALPR Administrators shall maintain a list of authorized users, who will be required to undergo training prior to obtaining access to ALPR information. If an authorized user changes job classifications to a position that is not authorized, the user's access to ALPR information shall be terminated and the user will be required to re-apply for authorization. If the user has not accessed ALPR information in 12 months or more, the user will also have to undergo training again prior to being approved to access ALPR information.

Only staff whose current work assignments require access to ALPR data shall be given access, subject to appropriate approval and training.

Accounts that have become inactive (i.e., if the account is not used to access ALPR information for 12 months) will be suspended after that 12-month time period. Approval to allow a DOJ employee to access ALPR information must be reviewed annually. When an authorized user leaves their employment with the DOJ, that user's account shall be deleted.

Prior to being given access to ALPR information, the user must provide the purpose for seeking ALPR information each time the system is accessed. The purpose provided by the user cannot be "investigation" alone; rather, the user must specify the specific investigation, for example, by referencing an internal case number, the code section being investigated, and/or including the last name of the target suspect. Users shall not include criminal history information or personal identifying information of a target suspect (beyond the suspect's last name), or any other information obtained from the California Law Enforcement Telecommunications System. Additionally, the user must specifically identify the employee for whom the search is being conducted, for audit purposes.

429.5 TRAINING

DOJ employees who are authorized to access ALPR information must undergo training regarding the appropriate use of ALPR information and privacy safeguards necessary to protect the privacy and civil liberties of California residents. The ALPR Administrators shall ensure that DOJ employees authorized to access ALPR information receive this training prior to obtaining access to ALPR information, and repeated thereafter once every two years, for as long as the employee is given access to such information. In the event that changes in technology and/or governing law renders retraining necessary, such retraining should be conducted as soon as reasonably possible.

429.6 SECURITY

As described in Section 429.4 above, the DOJ shall strictly limit access to ALPR information to persons who need the data for an authorized purpose and are approved by the ALPR Administrator to access ALPR information. Approval to allow an employee to access ALPR information shall be reviewed annually to ensure there is still an ongoing need for access.

Additionally, as described in Section 429.8 below, the DOJ will conduct annual audits assessing the access, use, and sharing of ALPR information, to ensure that ALPR information is accessed, used, and shared in accordance with statute and this policy.

429.7 PURPOSES OF, PROCESS FOR AND RESTRICTIONS ON SALE, SHARING OR TRANSFER OF ALPR INFORMATION

In accordance with Civil Code section 1798.90.55, subdivision (b), the DOJ shall not sell, share, or transfer ALPR information, except to another public agency (as defined in Civil Code section 1798.90.5, subdivision (f)) and only as otherwise permitted by law. As outlined above, “public agency” is defined as “the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency.” (Civ. Code, § 1798.90.5, subd. (f).) By definition, “public agency” does not include federal law enforcement agencies, out-of-state law enforcement agencies, or private entities.

Before sharing ALPR information with another public agency, the DOJ will verify and document a requesting agency’s purpose for obtaining the information and consider the requesting agency’s need for the information. The ALPR Administrator shall maintain a record of agencies that DOJ shares ALPR information with.

Any ALPR information downloaded or accessed by the DOJ must be maintained by DOJ in a secure location. If ALPR information is shared by email with other public agencies, the DOJ shall maintain a record of that transfer and maintain the original email in accordance with the DOJ’s records retention policies for criminal investigations.

In responding to a Public Records Act request or compulsory process in litigation seeking the production of ALPR information, DOJ will 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 DOJ “shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law.”

429.8 AUDITS

DOJ will conduct annual audits assessing the access, use, and sharing of ALPR information, to ensure that ALPR information is accessed, used, and shared in accordance with statute and this policy. The ALPR Administrator shall review and approve the audit results. Audit information shall be retained for three years. The ALPR Administrator shall ensure that the database it uses to query ALPR information conforms to this retention schedule.

429.9 RETENTION

ALPR information can only be accessed by authorized users with DOJ-issued computers, mobile phones, or smart devices, using at least dual factor authentication or similar security measures for any equipment used to access ALPR information. Any ALPR information downloaded, printed, or otherwise physically retrieved from an ALPR system shall be retained in accordance with the DOJ's records retention policies for criminal investigations.