POLICY
429

Automated License Plate Readers (ALPRs)

429.1 MISSION

This policy provides employees and the public with guidance regarding LAW ENFORCEMENT AGENCY'S collection, access, use, sharing, storage and retention of "automated license plate recognition" (ALPR) information, [and, if applicable: and maintenance of ALPR equipment]. LAW ENFORCEMENT AGENCY [if applicable: collects], accesses ALPR information, defined below, in order to further its mission of ensuring the public safety of California residents. In doing so, LAW ENFORCEMENT AGENCY is committed to complying with all applicable laws, including those laws related to the [if applicable: collection], 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 LAW ENFORCEMENT AGENCY'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 [LAW ENFORCEMENT AGENCY'S] policy.[1] (Civ. Code, § 1798.90.5, subd. (a).)

[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.

- 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 [LAW ENFORCEMENT AGENCY] 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.

[LAW ENFORCEMENT AGENCY's descriptive summary of the authorized purposes for which it accesses ALPR. This could include examples of how ALPR is typically accessed by the agency in the enforcement of laws (e.g., "including but not limited to X").]

[FOR AGENCIES THAT OPERATE AN ALPR SYSTEM:]

LAW ENFORCEMENT AGENCY operates an ALPR system. [*Agency should provide details regarding whether they use fixed or mobile cameras and how data is collected and stored*.]

[FOR AGENCIES THAT ALSO ACCESS ALPR SYSTEMS (i.e., THAT ARE ALSO END USERS)]

In addition to operating an ALPR system, LAW ENFORCEMENT AGENCY accesses ALPR information that is collected, not only by LAW ENFORCEMENT AGENCY'S ALPR system, but also ALPR information collected by other public agencies and private entities.

[FOR AGENCIES THAT DO NOT OPERATE AN ALPR SYSTEM BUT ACCESS ALPR INFORMATION COLLECTED BY OTHER AGENCIES:]

LAW ENFORCEMENT AGENCY 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 public agencies and private entities that operate ALPR systems. Because the LAW ENFORCEMENT AGENCY does not maintain an ALPR system but rather only accesses ALPR information that is collected by other agencies or entities, it is a considered an "end-user" of this information, and not an ALPR system operator.

---

(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).)

429.4 ADMINISTRATOR AND PERSONS AUTHORIZED TO ACCESS ALPR INFORMATION

Access to ALPR information is limited to employees or independent contractors who need the data for an authorized purpose. LAW ENFORCEMENT AGENCY shall designate an "ALPR Administrator," who shall be responsible for [*if ALPR system operator: collecting ALPR information and maintaining the ALPR system*], authorizing access to and use of ALPR information, and who shall be responsible for ensuring compliance with this policy and Civil Code §§ 1798.90.5, *et seq*. The ALPR Administrator shall have the classification of [*INSERT TITLE]*

The ALPR Administrator is responsible for authorizing the LAW ENFORCEMENT AGENCY's access to ALPR systems and is responsible for authorizing specific employees or independent contractors to access such ALPR information. [*Agencies to provide description of job title or other designation of employees and independent contractors authorized to access and use ALPR information [if only an ALPR end user], and/or, as applicable, a description of the job title or other designation of employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information [if the AGENCY is an ALPR system operator*].

Employees and independent contractors shall only be given access to the ALPR system for an authorized purpose, i.e., the enforcement of federal and California laws.

[*THE PROVISIONS BELOW ARE RECOMMENDED PRACTICES ONLY, NOT STATUTORY REQUIREMENTS.]*

The ALPR Administrator shall maintain a list of authorized users, who are 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 and undergo training again prior to be 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 an employee or independent contractor to access ALPR information must be reviewed annually. When an authorized user leaves the employment of the AGENCY or ceases being an independent contractor for AGENCY, 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, or suspect's last name. Users shall 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.

429.5 TRAINING

LAW ENFORCEMENT AGENCY employees and independent contractors who are authorized to access ALPR information must undergo periodic [*AGENCY TO INPUT SPECIFIC TIME PERIOD*] training regarding the appropriate use of ALPR information and privacy safeguards necessary to protect the privacy and civil liberties of California residents.

Such training shall be provided by [TBD LAW ENFORCEMENT AGENCY] prior to accessing the ALPR system or ALPR information, and repeated thereafter periodically [*AGENCY to provide specific time period*].

[BELOW IS SUGGESTED LANGUAGE, WHICH IS A BEST PRACTICE; THE SPECIFIC TRAINING REQUIREMENTS ARE SUGGESTIONS, AND AGENCY CAN PROVIDE OWN SPECIFICS RE TRAINING]:

Such training shall be provided by the [AGENCY TO PROVIDE WHO WILL PROVIDE TRAINING] prior to obtaining access to ALPR information, and repeated thereafter *AGENCY TO INPUT SPECIFIC TIME PERIOD*], 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.

If an employee's access is de-activated and later re-activated, the employee will be required to undergo training prior to being provided access to ALPR information.

429.6 SECURITY

[*Although a written contract between AGENCY and third-party vendor that stores AGENCY's ALPR information is not required by statute, the following language provides best practices for such contracts. SB 34 requires that any end-user or operator policy contain "a description of how the ALPR system will be monitored to ensure the security of the information." An end-user policy must also contain a process for periodic system audits.]*

> *[FOR AGENCIES THAT OPERATE AN ALPR SYSTEM AND ALSO ACCESS ALPR SYSTEMS (i.e., THAT ARE ALSO END USERS):]*

AGENCY must have a written contract with any ALPR system operator or third-party vendor hosting any ALPR information that AGENCY collects and provides to third-party vendors or other agencies to host. Any such contract must contain provisions that any ALPR system operator or third party that hosts ALPR information comply with all applicable laws regarding the collection, storage, use, access, sharing and retention of any ALPR information. Additionally, any such contract should also specify that LAW ENFORCEMENT AGENCY owns the data it uploads into the ALPR system, that the LAW ENFORCEMENT AGENCY's data will not be

stored outside of the United States or Canada, and that employees at the third-party vendor hosting LAW ENFORCEMENT AGENCY's data who have access to unencrypted ALPR information will undergo training and background checks.

This contract will also provide that the ALPR system operator or third-party vendor conduct periodic audits of its ALPR system or the hosting service to ensure the security of the ALPR information collected and stored. Any such contract with third-party vendors or ALPR system operators must include policies regarding any data security breaches that may occur.

Additionally, as described in Section 429.4 above, AGENCY shall strictly limit its own 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 or independent contractor to access ALPR information must be reviewed annually to ensure there is still an ongoing need for access. Further, as described in Section 429.8 below, AGENCY will conduct annual audits assessing its own access, use and sharing of ALPR information, including any hot lists (i.e., stored lists of vehicles of interest), to ensure that such information is accessed, used, and shared in accordance with statute and this policy.

FOR AGENCIES THAT DO NOT OPERATE AN ALPR SYSTEM BUT ACCESS ALPR INFORMATION COLLECTED BY OTHER AGENCIES:]

As described in Section 429.4 above, AGENCY shall strictly limit its own 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 or independent contractor to access ALPR information must be reviewed annually to ensure there is still an ongoing need for access. Additionally, as described in Section 429.8 below, AGENCY will conduct annual audits assessing its own access, use and sharing of ALPR information, including any hot lists (i.e., stored lists of vehicles of interest), 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), AGENCY 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, subdivision (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, including sharing of AGENCY'S ALPR information through a third-party vendor hosting platform, AGENCY shall verify and document a requesting agency's purpose for obtaining the information and consider the

requesting agency's need for the ALPR information. The ALPR Administrator shall maintain a record of agencies that AGENCY shares ALPR information with.

Any ALPR information downloaded or accessed by AGENCY must be maintained by AGENCY in a secure location. If ALPR information is shared by email with other public agencies, AGENCY must maintain a record of that transfer and maintain the original email for XXX [*LEA to Input Time Period; suggested practice is to maintain records in accordance with retention policies for criminal investigations*].

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

429.8 AUDITS

LAW ENFORCEMENT AGENCY must conduct periodic audits [AGENCY TO INPUT TIME PERIOD; SUGGESTED PRACTICE IS AT LEAST ANNUALLY] to [FOR ALPR OPERATORS: ensure the accuracy of ALPR information, correct any data errors, ensure that AGENCY's data is being accessed only by authorized agencies, and ensure compliance with data retention policies], and [for ALPR END USERS: to ensure ALPR information is accessed, used, and shared in accordance with statute and this policy. [*AGENCY to identify the person(s) responsible for performing those audits, who will review and approve the audit results, and how long audit documents will be retained. RECOMMENDATION IS THREE YEARS.*]

429.9 RETENTION

ALPR information can only be accessed by authorized users with LAW ENFORCEMENT-AGENCY-issued computers, mobile phones, or smart devices. Authorized LAW ENFORCEMENT AGENCY personnel are permitted to download ALPR information with LAW ENFORCEMENT-AGENCY-issued smart devices, mobile phones, and/or computers. LAW ENFORCEMENT AGENCY shall implement at least dual factor authentication or similar security measures for any equipment used to access ALPR information.

Any ALPR information downloaded or otherwise shared or printed must be destroyed within XXXX. *[LEA to input Retention Period]*

[FOR AGENCIES THAT OPERATE AN ALPR SYSTEM]

ALPR information uploaded to an ALPR system is maintained for a period of [Enter timeframe, e.g., 60 days to 6 months depending on how agency intends to use this information] unless the information is actively being used in an ongoing investigation or as evidence. Hot lists (i.e., stored lists of vehicles of interest) uploaded to an ALPR system shall be maintained for a period of [*enter appropriate timeframe*] and then manually deleted.

429.10 ALPR SYSTEM OPERATOR REQUIREMENTS FOR MAINTAINING RECORDS

As an operator of an ALPR system, [LAW ENFORCEMENT AGENCY] is required, if it accesses or provides access to ALPR information (regardless of whether it maintains custody of the ALPR system, for example, by maintaining it on its servers, or whether a third-party such as a private vendor hosts the LAW ENFORCEMENT AGENCY'S ALPR information on its database), to ensure that the ALPR information being accessed is used only for the authorized purposes described above.

To ensure that this ALPR information is used only for authorized purposes, the LAW ENFORCEMENT AGENCY must also maintain a record of any access given to its ALPR information; this record must include, at a minimum, the following:

(1) The date and time the information is accessed.

(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

[LEA to input: How long should that record be retained by the LEA? In what format? By whom?]