5-09/550.05 - Automated License Plate Recognition (ALPR) Privacy Policy

The purpose of this privacy policy is to ensure that all activities of the Los Angeles County Sheriff's Department (Department) and its personnel involving the capture, use, retention, and disclosure of information obtained through the Automated License Plate Recognition (ALPR) System comply with all applicable Federal, State, and County laws.

ALPR technology is a valuable law enforcement tool that when used appropriately, greatly enhances public safety. As with any law enforcement capability, its use must remain consistent with the United States Constitution, including the Fourth Amendment, and other applicable statutory authorities.

The Department affirms its obligation to fully comply with the statutes, regulations, and policies that govern the collection, retention, and disclosure of ALPR data, as well as with requirements for notification in the event of a data breach.

I. Authorized Purposes for Use of ALPR Technology

Pursuant to California Civil Code section 1798.90.51(b)(2)(A), the Department shall ensure that the use of ALPR technology and the collection of ALPR data are limited exclusively to the following authorized public safety purposes:

- Investigation for prosecution or exoneration of suspected criminal (including terrorist) incidents.
- Identification and/or location of wanted persons.
- Enforcement of sanctions, orders, or sentences.
- Crime prevention and legitimate law enforcement purposes.
- Crime analysis.
- Investigatory leads in subsequent investigations.
- Lifesaving efforts and critical missing persons.

II. Persons Authorized to Use or Access ALPR Technology/Data

Designated personnel who have been appropriately trained in the use of ALPR technology may access and query ALPR data as part of their official duties. Sworn personnel and designated civilian personnel whose duties require such access (e.g., crime analysts) shall have general user-level access to the Department's ALPR database for the purpose of querying information.

Information collected via ALPR technology may be analyzed only by qualified personnel who have successfully completed a background check, possess the appropriate security clearance, and have been approved and trained for that level of access.

Sworn personnel and designated civilian personnel assigned to the Advanced Surveillance and Protection (ASAP) Unit and the Sheriff's Data Network Unit, whose duties require such access, shall have administrator-level access to the Department's ALPR database. Administrator-level access authorizes these personnel to manage and control:

- The information available to each user group or classification of users.
- Specific data and system sites accessible to a user class, including data utilized in particular investigations.
- Sharing and interoperability functions with other authorized public agencies.
- Administrative and functional permissions necessary to maintain, control, administer, audit, or otherwise manage ALPR data and equipment.

III. Guidelines Regarding Appropriate Use

ALPR data must be collected in a fair and lawful manner during the routine duties of law enforcement in compliance with California Civil Code sections 1798.90.5 through 1798.90.55.

The Department shall not seek or retain information about individuals or organizations solely on the basis of religious, political, or social views or activities; participation in a noncriminal organization or lawful event; or race, ethnicity, citizenship, national origin, age, disability, gender, gender identity, or sexual orientation.

Department members shall use information-gathering and investigative techniques that are objectively reasonable under the totality of circumstances, consistent with applicable law and Department policy, and proportionate to the authorized law enforcement or administrative purpose.

ALPR data shall only be used for authorized law enforcement or job-related purposes. Data shall not be used for any non-work related purpose, and all access and use shall respect and safeguard the privacy, civil rights, and civil liberties of individuals.

All access controls, authentication requirements, purpose limitations, and retention practices shall fully comply with all applicable State laws governing the use of ALPR systems, including but not limited to California Civil Code sections 1798.90.5-1798.90.55 added pursuant to Senate Bill 34 and Government Code sections 7282-7284.12 revised pursuant to Senate Bill 54.

IV. Quality Assurance

The Department will investigate in a timely manner alleged errors and deficiencies (or will refer them to the originating agency) to correct, or refrain from using protected information found to be erroneous or deficient. Original data will not be altered, changed, or modified.

The Department will make every reasonable effort to ensure that information retained is derived from credible and reliable sources which convey accurate, current, and complete information, including the relevant context in which the information was sought or received.

The labeling of retained information (commonly referred to as hotlist information) will be evaluated by the Department or the originating agency when new information is gathered that may impact the reliability (content validity/software misread) of previously retained information.

The Department will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure the information from the ALPR System is updated and correct.

V. Sharing and Disclosure

All references in this policy to the term *public agency* are in accordance with the definition of public agency in California Civil Code section 1798.90.5(f). Specifically, a public agency "means 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."

Pursuant to California Civil Code section 1798.90.55(b), the Department shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law. The statute further states the provision of data hosting or towing services shall not be considered the sale, sharing, or transfer of ALPR information. Data sharing with other public agencies is subject to limitations and regular review to ensure compliance with the law and the protection of individual privacy rights.

Information gathered or collected, and records retained by the Department may be accessed or disclosed for legitimate law enforcement, criminal justice, or public safety purposes only to persons or entities authorized by law to have such access and only for those uses and purposes specified by law. The Department shall not confirm the existence or nonexistence of ALPR information to any person or agency that is not eligible to receive the information unless otherwise required by law.

An audit trail sufficient to identify who accessed or received ALPR information, the nature of the information requested or accessed, and the specific purpose of access will be retained by the Department for a minimum of two (2) years.

Any disclosure of ALPR data must undergo documented review and receive written authorization by the Department's designated Custodian of Records.

ALPR information gathered or collected, and records retained by the Department will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed or published without authorization.
- Disseminated to persons not authorized to access or use the information.
- Disclosed, transferred, or otherwise made available for civil immigration enforcement purposes, except when disclosure is expressly required by State or County law or pursuant to a judicial warrant.

The Department shares ALPR data with other public agencies as defined in California Civil Code section 1798.90.5(f), and only upon the execution of an inter-agency agreement by which each agency agrees that all

ALPR data will be gathered, accessed, used, and disclosed in accordance with applicable law, and further agrees:

- ALPR data shall be available only to authorized users for legitimate law enforcement purposes.
- Reasonable efforts will be made to ensure the accuracy of ALPR data.
- Shared hotlist data will not be stored for more than 24 hours without refresh.

All inter-agency agreements shall include a sunset clause requiring review and renewal of the agreement terms at least annually, and more frequently if circumstances require. Prior to renewal, the Department will review each agency's application for renewal of continued data sharing to confirm compliance with current laws and policies, and will verify that the partnering agency has not been identified by the California Attorney General's Office for non-compliance with SB 34 (automated license plate recognition systems).

VI. Information Retention and Destruction

These data retention and destruction requirements apply to ALPR systems managed and operated by the Department.

In general, ALPR data recorded or retained by the Department shall be retained for a period of two (2) years. After two years, ALPR data will be logically archived. Logical archiving means the record is flagged in the database as archived and can no longer be viewed or accessed by ALPR users but may be queried by an ALPR System Administrator.

If ALPR data is determined to have evidentiary value in a criminal or administrative investigation, the investigator shall submit a written request through their chain of command to the ALPR System Administrator requesting that the information be retained beyond the two-year period. The request shall include the case number, the specific reason for the retention, and the investigator's contact information. Once approved by the investigator's supervisor, the ALPR System Administrator shall ensure the requested information is retained until authorized for deletion.

ALPR data may be accessed beyond the two-year period under the following circumstances:

- When ALPR records related to a prosecution will be maintained until final disposition has been reached in the case.
- When ALPR records are included in a criminal case file, they shall be retained for the maximum period associated with that record type.
- When ALPR records are associated with an ongoing criminal investigation, they shall be retained in accordance with the applicable record retention schedule for that investigation.
- Whenever otherwise directed by a Department executive for a particular case or internal investigation, with the written concurrence of the concerned Division Chief or Division Director.

The Department retains the right to remove ALPR data earlier, based on limitations of data storage requirements and other technological or logistical considerations.

VII. Training

Field Operations Directive 09-004 establishes procedural guidelines and defines the responsibilities of personnel and units utilizing the ALPR system. Training staff at all stations shall be provided with and briefed on these procedures regarding ALPR equipment operation and system access requirements. All personnel authorized to use or access ALPR technology shall receive all relevant policies, directives, and procedures and are accountable for knowledge and compliance with them.

Formal training classes are provided on the authorized search engines used to access and query ALPR data. Training is also conducted by station training personnel and the ASAP Unit. The basic ALPR software interface is designed to be intuitive, and specific queries may only be conducted after the required information is entered, including the search purpose and the identifying information of the individual conducting the search. Detailed help tutorials are also available within the ALPR software to assist users.

All Department personnel with ALPR system access shall complete training that covers the privacy requirements of SB 34, the restrictions on immigration cooperation under SB 54, and the provisions of the Department's ALPR policy. Training on newly enacted ALPR related laws shall be provided as necessary. Annual refresher training shall also be required.

VIII. Accountability

All personnel authorized to use or access ALPR technology or data will be accountable for knowledge of this policy.

Department members shall report errors and suspected or confirmed violations of Department policies relating to protected information to their supervisor with the rank of sergeant or higher, or manager.

All access to the system will be logged, and the Department will maintain an audit trail of each instance of access or query, including the date and time the information is accessed, the license plate number or other data elements used to conduct the query, the username of the person accessing the information and, as applicable, their affiliation with the Department, and the purpose for accessing the information, in accordance with California Civil Code section 1798.90.52. Periodic random audits will be conducted to ensure and evaluate compliance with system requirements and with the provisions of this policy and applicable law.

IX. Audits

Audits shall be conducted at least annually, and more frequently if circumstances require. Audits shall include a review of a representative sample of individual user queries to assess whether each query was necessary for the investigation or case cited by the employee.

Audit trails will be maintained by the Department for a minimum of two (2) years.

The Department will annually conduct an inspection of the audit information contained in its database system,

which will be performed by the ASAP Unit. The ASAP Unit has the option of conducting random inspections, without announcement, at any time and without prior notice. The inspection will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Department's information system(s).

X. Oversight Reporting

In addition to the annual audit, the Department shall provide the Office of Inspector General, the Civilian Oversight Commission, and the Board of Supervisors with a semi-annual written report summarizing ALPR data or system access logs. The Department will submit these reports within 90 days after the end of the second quarter and within 90 days after the end of the fourth quarter of each calendar year.

Reports submitted to the Office of Inspector General will be unredacted. Reports submitted to the Civilian Oversight Commission shall be redacted only as legally necessary. A summary of each semi-annual report shall also be published on the Department's public transparency website.

In addition to the semi-annual reports, the Department shall prepare and transmit to the Office of Inspector General and the Civilian Oversight Commission an annual report summarizing ALPR training completions for the preceding year. The report shall confirm the number of personnel trained, the number of personnel who have completed refresher training, and any compliance issues identified. The Department will send the report to the Office of Inspector General and the Civilian Oversight Commission within 90 days after the end of the calendar year.

XI. Custodian of ALPR System and Records

The ASAP Unit shall have primary responsibility for maintaining and operating the ALPR database. This includes coordinating with personnel and public agencies that receive, request, or evaluate ALPR information, as well as overseeing the quality, analysis, destruction, sharing, and disclosure of ALPR data. The ASAP Unit will serve as the Department's Custodian of Records for the ALPR System and all associated data.

The Custodian of Records shall review and provide written authorization for any permissible disclosure of ALPR data, consistent with Section V of this policy. The Custodian of Records shall also maintain a record of each data request, including the requesting entity, and the basis for the request. These records shall be preserved in a manner sufficient to support audits, oversight reporting, and compliance reviews.

In addition, the Custodian of Records shall ensure compliance with data retention requirements described in Section VI, including logical archiving, permanent deletion, and verification of extended retention requests. The Custodian of Records shall ensure that all disclosures of ALPR data are made only to authorized entities and for authorized purposes as required by State or County law, or pursuant to a judicial warrant.