



Surveillance Use Policy

Automated License Plate Reader (ALPR) Data
San Diego Police Department

PURPOSE

ALPR data is a component of the San Diego Police Department's crime-fighting strategy that involves the identification of vehicles associated with suspects, witnesses, or victims. ALPR data enhances the Department's ability to focus its investigative resources, deter the occurrence of crime, and enhance public safety.

USE

The use of and access to ALPR data shall be for official law enforcement purposes only.

Legitimate law enforcement purposes include, but are not limited to:

- Locating vehicles that are stolen, wanted, under investigation, or associated with suspects, witnesses, or victims of a violent crime.
- Enhancing coordinated responses to critical incidents and public threats (e.g., active shooter, terrorism events).
- Safeguarding community members by locating at-risk missing persons, including through Amber, Silver, and Feather Alerts.

Only authorized users can access the ALPR databases. The users are primarily assigned to investigative and patrol units and have been vetted and approved by the Department's ALPR Program Administrator as having an investigative need for the technology.

In addition to ALPR data collected by SDPD, the San Diego Police Department also has access to ALPR data obtained from other agencies/companies that share their data with the ALPR databases. It is an analytic tool to help investigators review data returns from a variety of ALPR databases to enhance their investigations.

The following uses of ALPRs shall be expressly prohibited:

- To be used in a discriminatory manner and to target protected individual characteristics, including race, color, ethnicity, religion, national origin, age, disability, gender (to include gender identity and gender expression), lifestyle, sexual orientation, or similar personal characteristics, in accordance with Department Policy 9.31.
- To harass, intimidate, or discriminate against any individual or group.
- To violate any Constitutional rights, federal, state, or local laws (e.g., SB 34, California Values Act, AB 1242, etc.)
- To be utilized for any personal purpose.
- To investigate parking violations or conduct traffic enforcement.
- To view ALPR images or data without investigative or administrative need.

This Use Policy only applies to external ALPR data.



Surveillance Use Policy

Automated License Plate Reader (ALPR) Data San Diego Police Department

Department Procedures associated with the use of ALPR data include:

- DP 1.51- License Plate Recognition
- DP 4.13- Retention / Custody of Officer Notes, Documents, and Other Evidence.
- DP 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks.

DATA COLLECTION

ALPR data is obtained from law enforcement agencies, commercial providers, and private entities (e.g., shopping centers and Homeowners Associations (HOA) which collect data using ALPR technology.

DATA ACCESS

The San Diego Police Department shall designate in writing the personnel authorized to have access to the system, and the designation shall ensure that their access to and use of the images and data complies with federal, state, and local laws, including the TRUST Ordinance, as well as applicable Department procedures.

Personnel using ALPR technology shall be specifically trained in its operation and authorized by the Chief of Police or their designee. Authorized users include personnel listed in Department Procedure 1.51. The Department may grant access to supervisory staff of authorized users (i.e., sergeants, lieutenants, and captains) to ensure users comply with the Use Policy and Department Procedure.

Recorded data and images may be reviewed in accordance with the following criteria:

- By a Department employee conducting an official investigation.
- By members of the City Attorney's Office or Risk Management in connection with pending litigation.
- Pursuant to lawful process or by court personnel otherwise authorized to view evidence in a related case.
- As part of Department-approved training.

Authorized users under investigation for misconduct or criminal actions related to ALPR shall have their access revoked for the duration of the investigation.

DATA PROTECTION

The San Diego Police Department shall store images and data collected and retained as evidence from ALPR technology in compliance with the following Department Procedures:

DP 4.13 - Retention / Custody of Officer Notes, Documents, and Other Evidence.

DP 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks.

Encryption, firewalls, authentication, and other reasonable security measures shall be utilized to protect ALPR images and data.



Surveillance Use Policy

Automated License Plate Reader (ALPR) Data San Diego Police Department

All authorized users of ALPR technology shall access the system only through a login/password-protected system capable of documenting all access to information by name, date, and time.

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment, selecting, and approving technology solutions.

DATA RETENTION

ALPR data retained for an investigation shall comply with Department Procedure 3.02.

Any violations of the Use Policy identified through these audits will be reviewed and addressed, and appropriate corrective action will be taken as needed.

PUBLIC ACCESS

The San Diego Police Department considers all data and images downloaded from the ALPR and retained as evidence to be investigative records and are for official use only.

Upon public request, the system program administrator will provide all publicly disclosable information.

The San Diego Police Department will comply with all relevant Constitutional rights, federal, state, or local laws concerning any public requests related to the release of images and data from ALPR, including their availability to members of the public via the California Public Records Act (CPRA) process and by criminal defendants utilizing the discovery process as prescribed by law.

THIRD PARTY DATA SHARING

The San Diego Police Department only shares ALPR data with other California law enforcement agencies for legitimate law enforcement purposes, with the San Diego City Attorney or the San Diego District Attorney in connection with legal proceedings, or in response to a valid California court or judicial order, all in accordance with this Use Policy.

SDPD shall not:

- Share data with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies, in accordance with Senate Bill 34.
- This includes a prohibition on voluntarily sharing ALPR images or data with Immigration and Customs Enforcement (ICE), Border Patrol, or any other law enforcement agency for the purpose of enforcement immigration laws, as required by California Government Code section 7284.6 – The California Values Act.
- This also prohibits sharing ALPR images or data with any federal task forces.
- Release ALPR images or data to aid in the prosecution of an individual for providing, obtaining, or assisting in the provision or obtention of an abortion or any reproductive care, in accordance with the California FACE Act and the Reproductive Rights Law Enforcement Act.
- Sell ALPR data obtained or received by SDPD.



Surveillance Use Policy

Automated License Plate Reader (ALPR) Data
San Diego Police Department

TRAINING

All personnel authorized to access ALPR data shall receive annual training in the accessing and usage of any ALPR database by the program administrator and subject matter experts approved by the Department.

All employees who utilize ALPR databases shall be provided a copy of this Surveillance Use Policy, along with instruction on the constitutional protections (e.g., Fourth Amendment, etc.) and case law requirements associated with its use.

AUDITING AND OVERSIGHT

The program administrator shall maintain a list of personnel who are authorized to have access to the system. The authorization document shall ensure that their access to and use of the ALPR technology comply with federal, state, and local laws, the TRUST Ordinance, and applicable Department policies and procedures.

A log shall be maintained that records when access to ALPR images and data is requested. This shall include the date, time, data record accessed, staff member involved, case or event number, and purpose of the request. The log shall be available for presentation for all required audits, the annual report, and internal investigations. The program administrator will maintain oversight.

The program administrator, who holds a supervisory rank, shall conduct ALPR system audits monthly.

Audits include:

- Confirming compliance with state and local laws, including compliance with the Department's Use Policy
- Confirming users have current training and authorization to use the system
- Confirming that each search has a listed case number or incident number
- Confirming that complete case numbers and incident numbers are being used

During each audit, the program administrator shall check for case numbers that do not belong to the San Diego Police Department. Other California law enforcement agencies may provide case numbers upon request for a search or from outside agency wanted flyers. When this occurs, the program administrator conducting the audit shall verify the validity of the search.

Subject to the provisions of this policy, the Chief of Police or their designee has the discretion to prohibit the review of any data and images by Department employees if it is in the best interest of the Department or the City of San Diego.

MAINTENANCE

Vendors providing access to ALPR databases maintain the security and integrity of the ALPR data. ALPR data providers have systems designed with a variety of security tools, techniques, processes, and configurations that meet or exceed the Criminal Justice Information Services Division ("CJIS") requirements set forth by the FBI. All data transmissions and connections are made using secure connections.