



Surveillance Use Policy

Automated License Plate Recognition (ALPR) San Diego Police Department

PURPOSE

Automated License Plate Recognition Technology (ALPR) 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 enhances the Department's ability to focus its investigative resources, deter the occurrence of crime, and enhance public safety.

USE

ALPR systems have proven to be very effective tools in combating crime. The operation and access to ALPR data shall be for official law enforcement purposes only. The legitimate law enforcement purposes of ALPR systems include:

- Locating stolen vehicles, wanted vehicles, or vehicles subject to investigation and,
- Locating vehicles belonging to suspects, witnesses, and victims of a violent crime.

The San Diego Police Department will also use ALPR systems to enhance and coordinate responses to active critical incidents and public threats (e.g., active shooter, terrorist incident), safeguard the lives of community members by using this technology to locate at-risk missing persons (including responding to Amber, Silver, and Feather Alerts) and to protect assets and resources of the City of San Diego.

Any additional technologies, such as facial recognition or gunshot detection, will not be used in conjunction with ALPRs.

When alerted via ALPR that a vehicle is wanted, stolen, or of interest to law enforcement, the user must:

- (1) Visually ensure the plate was read properly and that the state of origin is consistent with the alert.
- (2) Confirm the alert status of the license plate information via the NCIC database. This can be accessed through a secure device (e.g., vehicle laptop, cellular phone, desktop computer, etc.) or by requesting the check through dispatch.

The following uses of ALPRs shall be expressly prohibited:

- To invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.
- 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 9.33.
- To harass, intimidate, or discriminate against any individual or group.
- To violate any Constitutional rights, federal, state, or local laws (e.g., California Values Act, FACE Act, etc.)



Surveillance Use Policy

Automated License Plate Recognition (ALPR) San Diego Police Department

- To be utilized for any personal purpose.
- To investigate parking violations and conduct traffic enforcement.
- To indiscriminately view video without investigative or administrative need.

Per Department Policy 1.01, all Department members shall comply with all Department Policies and Procedures and are subject to investigation and potential discipline for violations thereof.

Department procedures associated with the use of ALPR are:

- DP 1.49 Body Worn Camera/Evidence.com
- DP 1.51 Automated License Plate Recognition (ALPR)
- DP 3.02 Property Evidence
- DP 3.33 Smart Streetlights

DATA COLLECTION

The San Diego Police Department will 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 downloaded from the ALPR and retained as evidence by the Department are considered investigative records and are for official use only.

It is a violation of this policy to use ALPR technology to capture images and data of vehicles and license plates in a place where an expectation of privacy exists.

The National Crime Information Center (NCIC) is the primary database for the entry and management of wanted vehicles/persons that ALPR technology utilizes, along with Department hot plate/hotlists related to criminal investigations.

Proactive manual entry of ALPR hot plates/hot lists is permitted with license plate information (e.g., BOLO or AMBER alerts) in accordance with this Use Policy. It is the responsibility of the department member who creates the hot plate notification to manage, edit, and delete the plate as necessary.

Any camera adjustments or movements will comply with the Transparent and Responsible Use of Surveillance Technology ("TRUST") Ordinance.

All ALPR data collection, usage, retention, and release shall be in accordance with applicable State and Federal laws, including, but not limited to, California Civil Code 1798.90.51 through 1798.90.53, as further listed in Department Procedure 1.51.

DATA ACCESS

Personnel who are authorized to have access to the system shall be designated in writing, 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.



Surveillance Use Policy

Automated License Plate Recognition (ALPR) San Diego Police Department

Personnel using Automated License Plate Recognition (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. Access will also be granted to supervisory staff of authorized users (i.e., sergeants, lieutenants, captains) to ensure users are complying 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.
- The Chief of Police has the discretion to allow the viewing or release of data and images if they determine it is in the best interest of the Department.
- 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 and shall not have access restored until they have been cleared of wrongdoing.

DATA PROTECTION

Images and data collected by ALPR technology and retained as evidence shall be stored in a secured law enforcement facility with multiple layers of physical security and security protection. Encryption, firewalls, authentication, and other reasonable security measures shall be utilized to protect ALPR images and data.

All authorized users of ALPR technology shall access the system only through a login/password-protected system capable of documenting all access of 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. For additional details related to the IT governance processes, refer to the information at the following links:

- <https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf>
- <https://www.sandiego.gov/sites/default/files/legacy/humanresources/pdf/ar/ar9062.pdf>
- <https://www.sandiego.gov/sites/default/files/ar9063.pdf>
- <https://www.sandiego.gov/sites/default/files/legacy/humanresources/pdf/ar/ar9066.pdf>



Surveillance Use Policy

Automated License Plate Recognition (ALPR)
San Diego Police Department

- <https://www.sandiego.gov/sites/default/files/ar9068.pdf>
- <https://www.sandiego.gov/sites/default/files/ar9074.pdf>

DATA RETENTION

All ALPR images and data collected and stored on this technology platform shall be purged no later than 30 days from the date it was collected unless the data and image were determined to be evidence, downloaded, and stored pursuant to DP 3.02.

Special Projects and Legislative Affairs will be responsible for conducting a monthly audit to ensure the ALPR operating system is functioning correctly and that all data and images collected by the ALPR technology are appropriately purged.

PUBLIC ACCESS

DP 1.51 provides information 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. All data and images downloaded from the ALPR and retained as evidence by the Department are considered investigative records and are for official use only.

A log will be maintained by the Department to document when data and images from ALPRs were researched. The log will be provided by the system administrator upon public request, subject to certain exceptions.

The log will, at a minimum record general information about the incident that was investigated, along with the name of the investigator provided with the recorded images. A log entry that would reveal an ongoing investigation, or jeopardize public safety, will be withheld until this information may be safely released at the direction of the Chief of Police.

THIRD-PARTY DATA SHARING

All data and images collected from ALPR technology are considered investigative records for the Department and are for official Department use only. The following limitations apply:

- ALPR images and data shall never be voluntarily shared with Immigration and Customs Enforcement or, Border Patrol, or any other law enforcement agency, for the purpose of enforcing immigration laws, in accordance with California Government Code 7284.6 – The California Values Act.
- ALPR images and data shall never be released 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 California Penal Code 423.2, the California FACE Act and Penal Code 13778.2.



Surveillance Use Policy

Automated License Plate Recognition (ALPR) San Diego Police Department

- ALPR images and data shall never be shared with any federal task forces which involve in any manner the investigation or prosecution of federal crimes for conduct that is permitted under California law.
- ALPR images and data shall never be released to outside sources except the San Diego City Attorney and San Diego District Attorney in accordance with legal proceedings or of law enforcement agencies for the express purpose of investigating crimes in accordance with this Use Policy, until the adoption of a third-party data sharing use policy by the San Diego City Council.

Nothing in this Policy should be interpreted as limiting the use of collected data for legitimate purposes by prosecutors, judicial order, or other persons legally permitted to receive evidence under the law (See Public Access section above).

TRAINING

All personnel designated as system users shall receive training in the operation of ALPR technology by SPLA Unit personnel and subject matter experts approved by the Department.

All employees who utilize ALPR technology 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.

Training will include guidance on the use of ALPR technology and interaction with dispatch and patrol operations, along with a review regarding relevant policies and procedures. Training should also address applicable laws related to the use of video recording equipment and privacy.

All authorized users shall also complete annual refresher training as long as they are authorized to use ALPR technology. If there is a lapse in training, the SPLA Unit will revoke their access until they are in compliance.

The SPLA Unit shall keep records of all training provided to personnel authorized to use ALPR.

AUDITING AND OVERSIGHT

A list of personnel who are authorized to have access to the system shall be maintained by the SPLA Unit. 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, whether the request is internal or external to the San Diego Police Department. 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 internal and external audits, the annual report, and internal investigations. Oversight will be maintained by the SPLA Unit.



Surveillance Use Policy

Automated License Plate Recognition (ALPR)
San Diego Police Department

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

The San Diego Police Department shall maintain robust security procedures and practices, as noted in the Data Protection section above. These protections shall be in conjunction with those provided by the vendor. The vendor shall include operational, administrative, digital information technology security features and physical safeguards to protect ALPR images and data from unauthorized access, destruction, use, modification, or disclosure.

MODIFICATIONS TO THE USE POLICY

Prior to integration with other technologies, the requesting City department shall come to the City Council for public review and approval in accordance with the Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, section 210.0103.

Any modifications to this Policy must come to the City Council for public review and approval in accordance with the TRUST Ordinance, section 210.0103.