~~Second Modified~~ Surveillance Use Policy

Automated License Plate Recognition (ALPR)
San Diego Police Department

PURPOSE

Automated License Plate Recognition (ALPR) technology 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

The Department recognizes the importance of balancing public safety benefits with privacy and accountability. Accordingly, the operation of and access to ALPR data shall be for legitimate 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.

The Department ~~will~~ shall not integrate additional technologies, including facial recognition or gunshot detection, into ALPRs.

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

(1) Visually confirm that the ALPR system read the plate properly and that the state of origin is consistent with the alert.

(2) Confirm the alert status of the license plate information via the National Crime Information Center database. Access the database through a secure device (e.g., vehicle laptop, cellular phone, desktop computer, etc.) or request 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 9.313.

- To conduct a search of ALPR data based solely on past arrests, detentions, or history of police interaction.
- 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.

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
- DP 1.20 Overtime Compensation

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. The Department considers all data and images downloaded from the ALPR and retained as evidence to be 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.

The Department permits the proactive manual entry of ALPR hot plates/hot lists with license plate information (e.g., BOLO or AMBER alerts) in accordance with this Use Policy. Department members who create hot plate notifications are responsible for managing, editing, and deleting those plate entries as necessary.

Any camera adjustments or movements shall ~~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 1798.90.55, as further listed in Department Procedure 1.51.

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 and appeals process and shall not have access restored until they have been cleared of wrongdoing.

Access to the ALPR system outside the employee's scheduled work hours is prohibited unless approved in advance by the employee's immediate supervisor and done in compliance with Department Procedure 1.20.

DATA PROTECTION

The San Diego Police Department shall store images and data collected by ALPR technology and retained as evidence in compliance with Department Procedure 3.02 Property Evidence.

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 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.

In the event SDPD becomes aware of any breach that results in unauthorized sharing of personal information, SDPD shall notify all affected individuals in accordance with California Civil Code 1798.29. Additionally, SDPD will notify the Mayor and City Council members within 14 days.

Formatted: No underline, Font color: Auto

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.

An assigned program administrator 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.

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

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. 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 from the log described in the Auditing and Oversight section, subject to certain exceptions.

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 (Statutes of 2015, Chapter 532).
    - 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 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 California Penal Code 423.2, the California FACE Act and Penal Code 13778.2.
- Sell ALPR data obtained or received by SDPD.

The vendor or vendor subcontractor must immediately notify the City in writing, no later than 24 hours after being served with an out-of-state or federal warrant seeking access to San Diego's ALPR data. This notification must be sent to the Chief of Police, or their designee, and to the City Attorney, or their designee.

TRAINING

All personnel designated as system users shall receive training in the operation of ALPR technology by the program administrator 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.

The San Diego Police Department will provide training that includes guidance on the use of ALPR technology and interaction with dispatch and patrol operations, along with a review regarding relevant policies and procedures. The 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, access will be revoked until they are in compliance.

The program administrator shall keep records of all training provided to personnel authorized to use ALPR.

AUDITING AND OVERSIGHT

The program administration 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, 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. The program administrator will maintain oversight.

The program administrator, who holds a supervisory rank, will conduct ALPR system audits weekly.

Audits include:

- Confirming compliance with state and local laws, including compliance with the Department's Use Policy
- Confirming that equipment is functioning properly
- Confirming data is not being retained beyond the established retention period
- 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, and

During each audit, the system 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 system 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

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.