SAN DIEGO POLICE DEPARTMENT
PROCEDURE

DATE:	NOVEMBER 13, 2023
NUMBER:	1.51
SUBJECT:	AUTOMATED LICENSE PLATE RECOGNITION (ALPR)
RELATED POLICY:	N/A
ORIGINATING DIVISION:	SPECIAL PROJECTS AND LEGISLATIVE AFFAIRS (SPLA)
NEW PROCEDURE:	☐
PROCEDURAL CHANGE:	■ EXTENSIVE CHANGES
SUPERSEDES:	DP 1.51 - 7/08/2020

I. PURPOSE

This Department Procedure establishes guidelines for the responsible use of Automated License Plate Recognition (ALPR).

II. SCOPE

This procedure applies to all members of the Department.

III. BACKGROUND

ALPR is a computer-based information gathering system that utilizes specially designed cameras to rapidly capture an image of a vehicle license plate and convert the plate characters into a text file using optical character recognition technology. The text file can then be compared against pre-existing data files. If a match is found, the ALPR system user is notified by an alert. Because the ALPR system is programmed to check all vehicles in the same manner, it is an objective, non-discriminatory public safety tool. The data obtained by ALPR cameras is useful in criminal investigations.

All data and images gathered by the ALPR are for the official use of the Department. Because such data may contain confidential information, it is not open to public release without the consent of the Chief of Police of their designee.

IV. DEFINITIONS

ALPR technology - a searchable computerized database resulting from the operation of one or more fixed cameras combined with computer algorithms to read and convert images of vehicle license plates and characters they contain into computer-readable data (CA Civil Code 1798.90.5).

California Stolen Vehicle System (SVS) – The SVS is a state-wide computer system which is accessed by any terminal connected to the California Law Enforcement Telecommunications System (CLETS).

Information which can be uploaded to or received from the Department of Justice SVS computer includes:

- Stolen vehicle;
- Felony vehicle;
- Stolen identifiable vehicle parts;
- Stored vehicle;
- Impounded vehicle (to be entered to SVS under "Stored Vehicle Hold");
- Vehicles associated with missing persons;
- Repossessed vehicle;
- Lost vehicle; and
- License plate, lost or stolen.

Custom Hotlist - A Department-specific file that contains the license plate numbers of recently stolen vehicles, license plates of vehicles known to be associated with wanted or missing individuals, or descriptors of vehicles wanted in connection with a crime.

Data Breach –an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the San Diego Police Department. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure (CA Civil Code 1798.29).

Department of Justice (DOJ) Stop – A notification that states the listed vehicle is wanted as a stolen vehicle, wanted in connection to a felony crime or other law enforcement want.

Hotlist – A term referring to a list containing the license plate numbers of stolen vehicles; AMBER, SILVER, FEATHER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted or missing individuals. This may include information from the Department of Justice, the California Stolen Vehicle System (SVS), or other governmental repositories, and the Custom Hotlist.

"Hotplate" - A term referring to a license plate, from multiple sources, with a wanted status (e.g., stolen plates, stolen vehicles, and vehicles known to be associated with crimes). It can originate from a Custom Hotlist or Hotlist.

Personal Identifying Information (PII) – Is an individual's first name or first initial and last name in combination with various data elements, when either the name or the data elements are not encrypted, including information or data collected through the use or operation of an ALPR system, as defined in Section 1798.90.5. (California Civil Code sections 1798.29 and 1798.82)

V. PROCEDURES

A. Authorized Purposes, Collection, and Use of ALPR Data

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

    a. Locating stolen vehicles, wanted vehicles, or vehicles subject to investigation.

    b. Locating vehicles belonging to suspects, witnesses, and victims of criminal acts.

    c. Enhance and coordinate responses to active critical incidents and public threats (e.g., active shooter, terrorist incident)

    d. Safeguard the lives of community members by using this technology to locate missing persons (including responding to Amber, Silver, and Feather Alerts).

    e. To protect assets and resources of the City of San Diego.

2. ALPR Strategies

    a. Regular operation of ALPR should be considered as a force multiplying extension of an officer's regular patrol efforts to observe and detect vehicles of interest and specific wanted vehicles.

    b. ALPR may be legitimately used to collect data that is within public view but shall not be used to gather intelligence of constitutionally protected activities

NOTE: Department members shall not seek, submit, or retain license plate reader information about individuals, or an organization based solely on their religious beliefs, political affiliation, social views, activities, race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.

c. Reasonable suspicion or probable cause is not required for the operation of ALPR equipment.

d. **Users shall verify an ALPR response through CLETS before taking enforcement action.**

B. ALPR Operator Procedures

1. ALPR informational data files are periodically updated with different data sources being refreshed at different intervals. Therefore, it is important that ALPR users consider the potential for the lag time between the last update and an alert provided by the ALPR system on a vehicle of interest or wanted vehicle.

NOTE: Any alert provided by an ALPR system is to be considered informational and advisory in nature and requires further verification before action.

2. When alerted via ALPR that a vehicle is wanted, stolen, or of interest to law enforcement, the user should, to the fullest extent possible, take the following steps:

a. Ensure the plate was read properly and that the state of origin is consistent with the alert.

b. 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.

c. If the vehicle is confirmed stolen or wanted, officers shall, when safe to do so or via dispatch readback, review the DOJ Stop information to determine the nature of the advisory, including subsequent DOJ or DMV notifications, before taking any enforcement action.

3. In the event that sworn personnel are going to complete a vehicle stop on the information, and compelling circumstances are present or situational officer safety issues make it unsafe to confirm the status of the alert information

prior to taking action, the user must confirm the status of the alert information as soon as possible.

4. When action is taken on an alert vehicle (e.g. traffic stop, recovery, impound, etc.) it is the responsibility of the person taking action to provide the appropriate disposition information to the SPLA or Watch Commander's Office so the ALPR system (e.g. Hot Sheet, etc.) may be updated as necessary.

5. Only sworn law enforcement officers shall engage in contacting occupants of stolen or wanted vehicles.

C. Custom Hotlist Management

1. Proactive manual entry of the ALPR system Custom Hotlist is permitted with a license plate or vehicle description information when it meets an authorized purpose described in section V.A. of this procedure. All other entries shall be at the discretion of the SPLA Unit.

2. A Department member requesting to create a Custom Hotlist entry shall notify the SLPA Unit, (Monday through Friday between 0500 hours and 1600 hours on workdays), or the Watch Commander outside of the listed SPLA hours.

3. If an entry is no longer needed, the Department member who requested it shall immediately notify the SPLA Unit or Watch Commander to have the information deleted from the Custom Hotlist.

    a. Department members should notify the SPLA Unit or Watch Commander for any management or modification to their Custom Hotlist entries.

4. Training requirements regarding Custom Hotlist entries will be outlined in the SPLA Unit and Watch Commanders Operations Manuals and shall be followed by all authorized users.

5. When creating a Custom Hotlist entry, Department members should include all pertinent information (i.e., case number and type of crime). **Data such as Personal Identifiable Information (PII) should not be added to the hot plate.**

6. **Custom Hotlist entries will not be set as active for a period longer than 30 days.** Extension of a Custom Hotlist entry is permitted as long as it continues to meet the requirements. It is the responsibility of the requestor to notify the SPLA Unit or Watch Commanders Office prior to the 30 days if such an extension is necessary.

VI. DATA COLLECTION

A. 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.

B. 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.

C. 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.

D. 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.

E. Any changes to the use, purpose, or location of the ALPR technology, will comply with the Transparent and Responsible Use of Surveillance Technology ("TRUST") Ordinance.

VII. DATA STORAGE AND RETENTION

A. 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.

B. Special Projects and Legislative Affairs (SPLA) will be responsible for conducting a monthly audit to ensure the ALPR operating system is functioning correctly. A review of the data, via random sampling, will be conducted to confirm the accuracy of the data collected is consistent with the data confirmed during enforcement. If any consistent inaccuracies or issues are identified, SPLA team members will work the vendor to correct any such issues. SPLA will also confirm that all data and images collected by the ALPR technology are appropriately purged, in accordance with this procedure.

VIII. ALPR DATA ACCESS

A. 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.

B. Authorized users include select sworn and non-sworn personnel, such as Crime Analysts (backgrounded civilian non-sworn Department members) who enhance our investigations, specifically authorized by the Chief of Police or their designee.

C. 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. Access will 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.

D. Access will also be granted to staff of the Special Projects and Legislative Affairs Division, assigned as system administrators, to ensure authorized users are complying with authorized usage.

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

1. By a Department employee conducting an official investigation.

2. By members of the City Attorney's Office or Risk Management in connection with pending litigation.

3. Pursuant to lawful process or by court personnel otherwise authorized to view evidence in a related case.

4. Except when prohibited by law, 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.

5. As part of Department approved training.

F. 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.

IX. THIRD PARTY DATA SHARING

A. 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:

1. 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.

2. 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.

3. 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.

4. ALPR images and data shall never be released to third parties except the San Diego City Attorney and San Diego District Attorney in accordance with legal proceedings or law enforcement agencies for the express purpose of investigating crimes in accordance with this Department Procedure, until the adoption of a third-party data sharing use policy by the San Diego City Council.

5. Any disclosure of ALPR data to a third party shall comply with California Civil Code 1798.90.55

B. Nothing in this Department Procedure 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).

X. PROHIBITED USE

A. The following uses of ALPRs shall be expressly prohibited:

1. To invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

2. 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.

3. To harass, intimidate, or discriminate against any individual or group.

4. To violate any Constitutional rights, federal, state, or local laws (e.g., California Values Act, FACE Act, etc.)

5. To be utilized for any personal purpose.

6. To investigate parking violations and conduct traffic enforcement.

7. To indiscriminately view video without investigative or administrative need.

B. 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.

C. Any Department member who has knowledge concerning a violation of this procedure shall immediately report it for further investigation, in accordance with Department Policy 9.33.

XI. DATA PROTECTION

A. 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.

B. 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.

C. 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.

XII. DATA BREACH NOTIFICATION REQUIREMENTS

B. If the Department discovers a breach of the ALPR system that results in unauthorized third-party disclosure of personal information, the Department shall disclose the breach to all impacted individuals in accordance with California Civil Code 1798.29.

C. The notification shall be in the most expedient time possible and without reasonable delay, by providing a notification to those reasonably believed to have been affected by the breach.

D. The notification shall be titled "Notification of Data Breach" and will include the following information:

1. "What Happened"

2. "What Information Was Involved"

3. "What We Are Doing"

4. "What You Can Do"

5. "Other important information"

6. "For More Information" – A phone number or website to for further direction.

E. Per the law, at minimum the notification shall include:

1. Name and contact information for the department reporting the breach.

2. A list of the personal information subject to the breach.

3. Either the date, estimated date, or the date range that the breach occurred if the information can be determined when the notice is provided.

4. If notification was delayed as a result of law enforcement investigation.

5. A general description of the breach incident.

XIII. TRAINING

A. 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.

B. All employees who utilize ALPR technology shall be provided a copy of this Department Procedure, along with instruction on the constitutional protections (e.g., Fourth Amendment, etc.), CLETS certification, and case law requirements associated with its use.

C. 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.

D. 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.

E. The SPLA Unit shall keep records of all training provided to personnel authorized to use ALPR in accordance with California Civil Codes 1798.90.51 and 1798.90.53.

XIV. ALPR SYSTEM AUDIT AND OVERSIGHT

A. 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.

B. 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.

C. 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.