SAN DIEGO POLICE DEPARTMENT
PROCEDURE

DATE:	DRAFT
NUMBER:	1.51
SUBJECT:	LICENSE PLATE RECOGNITION
RELATED POLICY:	N/A
ORIGINATING DIVISION:	OPERATIONAL SUPPORT
NEW PROCEDURE:	☐
PROCEDURAL CHANGE:	■ EXTENSIVE CHANGES
SUPERSEDES:	DP 1.51 - 7/08/2020

I. PURPOSE

NEW

This Department Procedure establishes guidelines for the responsible and legal capture, storage and use of digital data obtained through the use of Automated License Plate Recognition (ALPR) technology.

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 audible alert and an associated notation on the user's computer screen. 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.

NEW

All unaltered data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

NEW

IV. DEFINITIONS

ALPR technology - a searchable computerized database resulting from the operation of one or more mobile or 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).

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)

Hotlist - A file that contains 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.

Hotlist Sources ALPR systems - used by law enforcement; can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists

Hotplate - A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

Personal Identifying Information (PII) – In accordance with California Civil Code sections 1798.29 and 1798.82, 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.

V. PROCEDURES

NEW

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, wanted, or subject of investigation vehicles.

b. Locating vehicles belonging to witnesses and victims of a violent crime.

c. Locating vehicles associated with missing or abducted children and at-risk individuals.

d. Visually marking parked vehicle locations to confirm parking enforcement violations.

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 protected First Amendment activities.

NEW

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. Use of ALPR-equipped cars to conduct license plate canvasses and grid searches is encouraged, particularly for major crimes or incidents, as well as areas that are experiencing any type of crime series.

NEW

e. ALPR-equipped vehicles should be deployed as frequently as possible to maximize the utilization of the system and used in conjunction with other available ALPR technology (e.g. Smart Streetlights), when possible.

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

B. ALPR User Procedures

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.

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:

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

NEW

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 requesting the check through dispatch.

    a. 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 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.

NEW

C. Hot Plate Management

1. The National Crime Information Center (NCIC) remains the primary database for the entry and management of wanted vehicles/persons.

2. Proactive manual entry of the ALPR system hot plates/hot lists is permitted with license plate information (i.e., BOLO or AMBER alerts) when it meets an authorized purpose described in section V.A. It is the responsibility of the department member who creates the hot plate notification to manage, edit, and delete the plate information from the ALPR system as necessary.

3. Additionally, strict adherence to the training regarding hot plate creation, as provided by the ALPR User Course, detailed in Section X of this procedure, will be maintained. When creating a hot plate, department members must 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.**

4. **Hot plates will not be set as active for a period longer than 15 days.** Re-entry of a hot plate is permitted as long as it continues to meet the standards for hot plate creation

VI. ALPR DATA STORAGE, RETENTION AND ACCESS

A. Authorized users of the ALPR system are: Detectives, who conduct in-depth criminal investigations; Officers, who are assigned to an area of patrol; RSVPs, who provide additional resources to the police department by assisting with crime prevention programs and promoting community awareness toward public safety; ALPR manufacturer service technicians who provide technical support for ALPR hardware and software and SDPD Information Services technicians who coordinate the development, testing, implementation, and modification of department information systems and provide hardware/software technical support to end users in the day-to-day operation of department systems.

NEW

1. Authorized users have access to additional data via the ARJIS website, and their specific security requirements. Access to the external system is controlled by ARJIS.

B. Requested Information Unit personnel will ensure personnel operating ALPR systems have the technical expertise and necessary department-approved training to access ALPR systems. Training requirements for users include CLETS certification, SDPD Procedure 1.51 compliance, and ARJIS training.

C. ALPR systems have the capacity to collect and store data relevant and necessary for authorized law enforcement purposes.

D. ALPR data stored in our system does not include any personally identifying information, or information which relates the license plate image to the driver or registered owner of a vehicle.

E. The Department will only use ALPR Technology to collect license plate data within public view. The Department will not use ALPR Technology for the sole purpose of monitoring individual activities that are otherwise protected by the First Amendment to the United States Constitution or the California Constitution.

NEW

F. All data collected by the department's ALPR system will be stored for a period not to exceed 30 days. After 30 days, the information will be automatically purged from the system.

NEW

G. This retention policy applies only to the ALPR information contained in the department's ALPR system. Once ALPR information is downloaded by department personnel and incorporated into a criminal intelligence record or an investigative case file, the ALPR information is then considered investigative information or intelligence and the laws, regulations, and policies applicable to that type of information govern its use.

NEW

H. Each authorized user is responsible for preserving the ALPR data that has evidentiary value to a criminal investigation through the use of the reporting feature found within the ALPR system. This data will be stored longer than the regular retention period. If the ALPR record is evidence in a specific criminal or other law enforcement investigation, the department authorizes the transfer of the applicable record from the ALPR system server to the department's case management system or in a form of digital storage media or report for preservation.

VII. RELEASING ALPR DATA

A. All electronic images or unaltered data gathered by ALPR technology are for the exclusive use of law enforcement personnel in the discharge of official duties and are not open to the public.

NEW

B. Department members shall not share ALPR data with commercial or private entities or individuals. However, sworn members may disseminate ALPR data to government entities with an authorized law enforcement or public safety purpose for access to such data, using the following procedures:

1. The government or law enforcement agency shall provide a written request for the ALPR data that includes:

   a. The name of the agency.

   b. The name of the person requesting.

   c. The intended purpose of obtaining the information.

2. The request shall be reviewed by the Chief, or an authorized designee, and approved before the request is fulfilled.

NEW

3. The approved request and the record of what was disclosed shall be retained on file by the Requested Information Unit for a period of two years.

NEW

4. No ALPR data shall be shared with any government agency, for the specific purpose of immigration enforcement, in accordance with California Government Code 7282.5.

C. Nothing in these guidelines should be interpreted as limiting the use of the electronic images or data for legitimate purposes by prosecutors, or others permitted to receive evidence under the law.

NEW

D. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55 and per any interagency agreements.

NEW

VI. VIOLATIONS

A. Unauthorized access to the system, misuse of the system, unauthorized reproduction of images, or unauthorized distribution of images shall result in an internal investigation and possible disciplinary or criminal action, consistent with the Public Safety Officers Procedural Bill of Rights Act and the appropriate employee organization MOU.

B. 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.

NEW

VIII. DATA BREACH NOTIFICATION REQUIREMENTS

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 sections 1798.29 and 1798.82. 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.

A. 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.

At minimum, the notification shall include:

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

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

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

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

D. A general description of the breach incident.

IX. ALPR SYSTEM ADMINISTRATOR ROLE AND RESPONSIBILITIES

NEW

The Special Projects Commanding Officer, or their designee, is the custodian of the ALPR program as required in California Civil Code 1798.90.51(b)(2)(E) and 1798.90.53(b)(2)(E). System Administrators who oversee the program shall be sworn members and are responsible for performing the following duties:

A. Ensuring personnel operating ALPR systems have the technical expertise, training, and necessary clearances to access law enforcement databases and information.

B. Updating users of any technological, legal, or other changes that affect the use of ALPR systems.

C. Controlling ALPR use, data access, and sharing of data with other authorized agencies.

D. Maintain user records containing query information including the purpose, date/time of access, data queried, and user identification in accordance with California Civil Code section 1798.90.52, which states:

1. If an ALPR user accesses or provides access to ALPR information, the ALPR user shall do both of the following:

(a) Maintain a record of that access. At a minimum, the record shall include all of the following:

(1) The date and time the information is accessed.

(2) The license plate number or other data elements used to query the ALPR system.

(3) The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.

(4) The purpose for accessing the information.

(b) Require that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.

E. Serving as the primary point of contact for regional ALPR issues and notification of system or operational changes.

F. Developing and delivering training for ALPR system use, including the initial training and any subsequent updates or revisions as necessary.

NEW **X. <u>ALPR SYSTEM SECURITY AND ACCURACY</u>**

A. All ALPR data downloaded to an ALPR system-accessible device or computer, and in storage, shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time, and purpose (Civil Code § 1798.90.52).

B. ALPR system audits shall be conducted on a regular basis by the Requested Information Unit. The purpose of these audits is to ensure the accuracy of ALPR Information and correct data errors.

C. Special Projects sworn personnel will monitor its use of ALPR technology to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process and time period system audits.

D. Special Projects personnel shall provide an annual report, consistent with the City of San Diego's Municipal Code, which contains following for the previous 12-month period:

1. The number of times the ALPR technology was used.

2. A list of agencies other than the San Diego Police Department that were authorized to use the equipment.

3. A list of agencies other than the San Diego Police Department that received information from use of the equipment.

4. Information concerning any violation of this policy.

5. Total costs for maintenance, licensing and training, if any.

6. The results of any internal audits and if any corrective action was taken. The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment

XI. ALPR USER COURSE / TRAINING

NEW

A. The Training Section shall ensure that members receive department-approved ALPR User Course training for those authorized to use or access the ALPR system and shall maintain a record of all completed trainings, in accordance with California Civil Codes 1798.90.51 and 1798.90.53.

B. Training requirements for employees authorized in ALPR use shall include completion of training by the Training Division or appropriate subject matter experts as designated by the San Diego Police Department Special Projects Division. Such training shall include:

1. Applicable federal and state law

2. Applicable policy

3. Memoranda of understanding

4. Functionality of equipment

5. Accessing data

6. Safeguarding password information and data

7. Sharing of data

8. Reporting breaches

9. Implementing post-breach procedures

C. Training updates are required annually.