Policy
453

Fresno Police Department Policy Manual

Automated License Plate Readers (ALPRs)

453.1 POLICY

The policy of the Fresno Police Department is to 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 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.

453.1.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates along with the vehicle make, model, color, and unique identifiers through the Department's ALPR system. The system is used by the Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. Additionally, it may be used to gather information related to active warrants, electronic surveillance, suspect interdiction, stolen property recovery, and active criminal investigations (e.g., Hot list, Hot plate).

ALPR shall not be used to intentionally invade the privacy of community members, nor will it be used in a discriminatory manner that targets individuals or groups.

ALPR shall only be used for legitimate law enforcement purposes. It provides data from one moment in time that must be weighed as only one piece of evidence in an investigation and corroborated by other facts.

453.2 DEFINITIONS

ALPR - A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

ALPR Administrator - The Special Response Division Commander serves as the ALPR Administrator.

ALPR Read/Detection – A single instance where an ALPR camera captures an image in a public place, and using an algorithm, detects and reads a license plate within the photo/video, and provides information regarding the location of the ALPR system at the time of the detection/read

ALPR Search – A query of stored ALPR data

Alert Hit - Alert from the ALPR system that a scanned license plate number maybe in the NCIC or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violence protective order, and statewide emergency alerts.

Hot List - A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, National Crime Information Center (NCIC), Department of Motor Vehicles (DMV), local BOLO's, etc.

Vehicles of Interest - Including, but not limited to, vehicles which are reported as stolen; display stolen license plates; vehicles linked to missing and/or wanted persons and vehicles flagged by law enforcement agencies.

Detection - Data obtained by an ALPR of an image (i.e., License plate) within public view that was read by the device, including potential images (i.e., the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

Flock Safety - A semi portable, self-sustaining ALPR camera and cloud-based storage system which holds license plate reads in a searchable database.

Motorola Solutions (Vigilant) - A mobile license plate recognition system, self-sustaining ALPR Cameras and cloud-based storage system which holds license plate reads in a searchable database.

453.3 ALPR ADMINISTRATION

The Special Response Division Commander or their designee shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code §1798.90.5 et seq. This includes but is not limited to (Civil Code §1798.90.51; Civil Code §1798.90.53):

(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information;
(b) Determining the locations for fixed ALPRs within the City of Fresno;
(c) Training requirements for authorized users;
(d) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws;
(e) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52;
(f) The title and name of the current designee in overseeing the ALPR operation;
(g) The retention and destruction of ALPR data; and
(h) Ensuring this policy is conspicuously posted on the department's website.

The Special Response Division Commander will assign members under their command to administer the day-to-day operation of the ALPR equipment and system administration.

453.4 AUTHORIZED USERS AND OPERATIONS

Use of the ALPR equipment and system is restricted to the purposes outlined below. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose (Civil Code §1798.90.51; Civil Code §1798.90.53).

(a) The ALPR system shall only be used for official law enforcement business using a Fresno Police Department case number related to an active investigation;
(b) An ALPR may be used in conjunction with any routine patrol operation, missing person, or criminal investigation. ALPR cameras can be used in public places and collect data without reasonable suspicion or probable cause;
(c) To conduct a search in the ALPR system, users must have a legitimate law enforcement purpose related to an active case;
(d) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates and unique vehicle identifiers reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles;
(e) No ALPR user may access department, state, or federal data unless otherwise authorized to do so;
(f) Officers should verify an ALPR response before taking enforcement action that is based solely on an ALPR alert;
(g) Only personnel who have received department-approved training and have been provided user

accounts shall use or access the ALPR system. (Civil Code § 1798.90.51; Civil Code § 1798.90.53);

(h) Supervisor approval must be obtained prior to a user being granted ALPR system access. Accounts will be granted on a need to know and right to know basis;
(i) Account usernames and passwords shall not be shared and only the assigned user may access their ALPR account; and
(j) User accounts will be immediately deactivated for any separated employees, inactive users (over 90 days), and users who no longer need the account or others as deemed necessary.

453.4.1 AUTOMATIC LICENSE PLATE READER NOTIFICATIONS

Officers may receive an ALPR Alert Hit from an ALPR system An Alert Hit alone shall not be a basis for police action (other than following the vehicle of interest).

Before any law enforcement action is taken because of an ALPR Alert Hit, the officer should verify an ALPR Alert Hit through NCIC, CLETS, or other law enforcement database. Once an Alert Hit is received, the officer should confirm that the observed license plate from the ALPR system matches the license plate of the observed vehicle.

Officers shall not take any police action that restricts the freedom of any individual based solely on an ALPR Alert Hit unless it has been validated. Because the ALPR Alert Hit may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. Prior to the initiation of a vehicle stop, an officer shall:

(a) Visually verify that the vehicle plate number matches the plate number run by the ALPR system, including both alphanumeric characters of the license plate and the state of issuance; and
(b) Verify the status of the plate through DMV.

453.4.2 HOT LIST/HOT PLATE

Hot List and Hot Plate retention will be set for no longer than 30 days. All hot list vehicles shall have an expiration date. Users are responsible for managing and maintaining the Hot List(s) or Hot Plate(s) they create in the system. Data entered into the ALPR system is limited to missing or at-risk person investigations and active criminal investigations where reasonable suspicion exists that a crime is being committed or has been committed. No CLETS data may be entered. Personnel will not enter any license plates into the Fresno PD Hot List unless the vehicle meets the above criteria. All hot list vehicles shall include:

(a) An FPD case number;
(b) Reason for the vehicle being in the system;
(c) Requesting officer's name;
(d) Requesting officer's contact information;
(e) Applicable instructions, (e.g., "P/C for arrest," "No P/C for arrest, stop only with P/C and identify occupants," "Do not stop, contact officer of Alert Hit," "R/O known to carry firearm," etc.); and,
(f) Other pertinent information.

453.5 DATA COLLECTION AND RETENTION

Department-owned ALPR data will not be retained longer than 30 days unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. ALPR data that is evidence to be used for criminal prosecution shall be stored in Evidence.com and retained for a period consistent with other types of evidence. Retention periods for ALPR data collected by commercial providers and/or other law enforcement agencies and made available to this department are set by those providers.

All ALPR data security features will comply with Federal Bureau of Investigation-Criminal Justice Information Services (FBI-CJIS) standards.

453.6 MONITORING AND ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Fresno Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code §1798.90.51; Civil Code §1798.90.53):

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code §1798.90.52);
(b) Members approved to monitor ALPR data use under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action; and
(c) ALPR system audits shall be conducted according to the guidelines below.

453.6.1 AUDITS

ALPR system audits will be conducted by the Special Response Division Commander or their designee to ensure the Fresno Police Department's ALPR systems meet the high standards and privacy expectations of the community. Audits will be utilized to ensure public confidence in the ALPR programs, identify and address unauthorized use of the system, ensure system data confidentiality, and ensure the programs are within CJIS compliance. The audit process will seek to ensure the ALPR systems are in compliance with California Civil Code §1798.90.5 and §1798.90.55.

ALPR systems audits will be conducted every 28 days and will include:

(a) A review of searches by 5% of randomly selected users who searched each database during the review period;
(b) A review of 5% of randomly selected searches in the Motorola database;
(c) A review of searches flagged by Flock Safety's AI-assisted auditing tool (Audit Assistance);
(d) A review of all the hot lists, hot plates, and freeform searches;
(e) A review of system administrator access;
(f) A review of agency settings for CJIS compliance;
(g) Confirmation that retention settings remain at 30 days;
(h) A review of data sharing access and confirmation that data has only been shared in compliance with law and policy; and,
(i) Deactivation of user accounts that have been inactive for more than 90 days.

Additionally, any quarterly audits will include:

(a) A review of data sharing MOUs and expirations dates;
(b) A review of training compliance for users and system administrators;
(c) A review of the Flock Safety Transparency Portal;
(d) Confirmation that the agency's current ALPR policy is posted on the City's website.

Any suspected misuse of the system shall be administratively investigated, with appropriate disciplinary and/or training action taken as needed.

Audit records will be maintained under the control of the Special Response Division Commander or their designee for a period of three years at which time they will be purged.

453.7 RELEASE OR SHARING OF ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Non-federal outside agencies requesting access to Department ALPR data that are within the state of California may request a Memorandum of Understanding (MOU) from the Special Response Division Commander that, once signed, will allow authorized members of their agencies to search FPD's ALPR data. No ALPR data shall be shared with federal and/or non-California agencies. Outside agencies that do not have a signed MOU for data

sharing must make a written request to the Special Response Division Commander that includes:

1) The name of the agency;
2) The name of the person requesting;
3) The intended purpose of obtaining the information; and,
4) The case or incident number associated with the request.

The approved written request and MOU are retained on file under the control of the Special Response Division Commander or authorized designee. MOUs shall be valid for one year from the date of execution and will be reviewed and renewed each year to continue the data sharing relationship.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Release of Records and Information Policy 810 (Civil Code §1798.90.55). The City Attorney's Office will review all requests for ALPR data.

GC § 7284.6 prohibits the use of Department resources solely for immigration violations. ALPR data shall not be used or shared for immigration related purposes.

453.8 ACCURACY AND DATA ERRORS

ALPR data is not personally identifiable information. A license plate number identifies a specific vehicle, not a specific person. Although a license plate number may be linked or otherwise associated with an identifiable person, this potential can only be realized through distinct investigative steps. Absent this investigative step, the license plate number and the time and location data attached to it are not personally identifying. Although ALPR systems automate the collection of license plate numbers, it is the investigation process that identifies individuals.

Officers will ensure the accuracy of the notification of a hit by comparing the scanned image to the system provided original case report results and verify an ALPR response through NCIC, CLETS, or other law enforcement database before taking enforcement action that is based solely on an ALPR alert.

453.9 DISCLOSURE OF DATA BREACH

Any data breach will be handled in accordance with Policy 810 Release of Records and Information which ensures compliance with Civil Code §1798.29.

453.10 TRAINING

The Special Response Division Commander should ensure that members receive department-approved training for those authorized to use or access the ALPR equipment and system (Civil Code §1798.90.51; Civil Code §1798.90.53). Refresher training regarding ALPR program updates and for reactivated users will be provided as needed.