Automated License Plate Readers (ALPRs)

404.1 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.

404.2 DEFINITIONS

Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

ALPR Operator: Trained Department members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

ALPR Administrator: The Operations Lieutenant or the Chief's designee, serves as the ALPR Administrator for the Department.

Hot List: A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA DMV, Local BOLO's, Silver and Amber Alerts etc.

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

Detection: Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the ALPR, including potential images (such as 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.

Hit: Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (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 violation protective order or terrorist-related activity.

404.3 POLICY

The policy of the University of California, Irvine Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing established privacy rights of the public.

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

404.4 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the University of California, Irvine Police 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. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Operations Lieutenant. The Operations Lieutenant will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

404.4.1 ALPR ADMINISTRATOR

The Operations Lieutenant 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) Training requirements for authorized users.

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

(d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(e) The title and name of the current designee in overseeing the ALPR operation.

(f) Working with the Custodian of Records on the retention and destruction of ALPR data.

(g) Ensuring this policy and related procedures are conspicuously posted on the department's website.

404.5 OPERATIONS

Use of an ALPR 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) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any criminal investigation.

(c) Partial license plates and unique vehicle descriptions reported during major crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.

(e) If practicable, the officer shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) and/or MDC before taking enforcement action. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Because the ALPR alert may relate to a vehicle and may not relate to

the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop).

(f) Training. No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.

(g) Login/Log-Out Procedure. To ensure proper operation and to facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.
Prohibited Uses: The ALPR system, and all data collected, is the property of the UC Irvine Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
2. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
3. Use Based on a Protected Characteristic. It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
4. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
5. First Amendment Rights. It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights. Anyone who engages in any prohibited use of the ALPR system or associated scan files, or hot lists may be subject to:
    (a) Criminal prosecution,
    (b) Civil liability, and/or
    (c) Administrative sanctions, up to and including termination.

404.6 CUSTOM HOT LISTS

ALPR Custom Hot Lists are ALPR user created lists of vehicles with associated information, actions, or requests to other ALPR users. Custom Hot Lists are an invaluable tool to assist law enforcement.

When using Custom Hot Lists, the following shall apply:

(a) Custom Hot Lists should generally be created by the primary investigating ALPR user or an authorized designee.

(b) Custom Hot List information shall be inputted on a department supplied form and approved by an immediate supervisor. Information will include:

1. Entering department member's name
2. Related case number
3. Short synopsis describing the nature of the originating criminal investigation
4. Entries may include attachments, such as law enforcement flyers, that contain further details of the crime or requests from the investigating ALPR user.

(c) UCIPD dispatchers or detectives will input the Custom Hot List information into the ALPR system.

(d) No user shall create a Custom Hot List accessible only to themselves. At minimum, each Custom Hot List shall include the creator's supervisor or any other supervisor tasked with ALPR usage audits.

(e) The creator is required to maintain, update, or remove entries as circumstances change, such as when the vehicle is no longer wanted or no longer suspected of a crime.

404.7 DATA COLLECTION, SECURITY AND RETENTION

The Operations Lieutenant is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data.

(a) ALPR records retained by the department will be maintained for a minimum of 90 days, safeguarded, and purged according to all applicable laws, policies and ALPR system provider limitations. ALPR information that may be needed for active or probable litigation, is the subject of an active public records request, or is needed for auditing purposes shall be maintained until the underlying matters are fully resolved before being destroyed.In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

(b) The University of California Irvine Police Department, or its authorized vendors, will retain raw ALPR information for a period not to exceed the lesser of the maximum period allowed by law, or the retention period established in applicable service agreements.

(c) Electronic data gathered during ALPR usage is the property of the University of California Irvine Police Department. The approved ALPR vendor will maintain responsibility for adherence to protocols involving information security in accordance with FBI CJIS security policy.

(d) Authorized department vendors with access to systems containing ALPR data shall maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.

(e) All ALPR login and query records will be retained for at least the minimum period required by law, unless the information has been timely requested for investigative or other legal reasons. Pursuant to Civil Code § 1798.90.52, any records retained must contain, at a minimum, the following information:

1. The date and time ALPR information was accessed.
2. The username of who accessed the information.
3. The license plate number or other data elements used to query the ALPR system.
4. The stated purpose for accessing the information.

404.8 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The University of California Irvine 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 access ALPR data 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.

(c) Department members shall only use their own assigned username and password when accessing any ALPR system.

(d) When conducting a specific license plate search of ALPR data, department members shall include a related case number for justification.

(e) When conducting a generic vehicle description search of ALPR data, department members shall include a justification description or related case number.

(f) Any printed ALPR information must be destroyed using a secure method. No materials shall be disposed of in regular trash or recycling containers.

(g) No ALPR data shall be given, sold, shared or otherwise transferred to any unauthorized party.

(h) ALPR system audits should be conducted on a regular basis. Sergeants assigned as ALPR administrators are responsible for the completion of monthly audits of ALPR queries performed by department personnel to include any Custom Hot Lists created by those users.

(i) Any violations of this policy may result in temporary or permanent revocation of access.

(j) Any breach or unauthorized or unintentional release of any ALPR information shall be immediately reported to the Operations Lieutenant.

This policy does not prohibit further restricting user access, revoking access without cause, or requiring supplemental training for assigned ALPR users.

For security or data breaches, see the Records Release and Maintenance Policy.

404.9 RELEASING 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, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Operations Lieutenant or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

404.10 TRAINING

The Training Manager should ensure that members receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).