Senate Bill No. 34

Automated License Plate Readers (ALPRs)

462.1 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.

462.2 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Alhambra 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 th Fleet Coordinator and Records Manager, under the oversight of the Field Services Assistant Chief. The Field Services Assistant Chief will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. Each section will assign personnel to be responsible for maintaining and updating their section's list of license plates entered into the ALPR system, also known as a "hot list." The Department shall utilize hot lists that further the specific goals of the ALPR system where there is a legitimate and specific law enforcement reason for identifying a vehicle or a person reasonably believed to be associated with that vehicle.

462.2.1 ALPR ADMINISTRATOR

The Field Services Assistant Chief 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 Records Manager on the retention and destruction of ALPR data.

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

Adoption Date: 2016/03/24

462.3 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 routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) 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 reported during major crimes should 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) No ALPR operator may access department, state or federal data unless otherwise authorized to do so.

(f) Hot List Administrators shall document the reason for manually entering a license platenumber into the ALPR system.

(g) The Field Services Assistant Chief may approve a mutual aid request to assist law enforcement from other agencies and share ALPR data when they become aware of a serious incident, as to which they reasonably believe the ALPR may be useful, as resources permit.

462.3.1 ALPR ALERT PROTOCOLS

When an ALPR alerts on a stolen vehicle the officer shall, prior to initiating a traffic stop or detaining the occupants of the vehicle:

(a) Verify that the ALPR has recorded the license plate number correctly

(b) Verify through CLETS/Dispatch that the car is currently reported as stolen.

1. Do this before stopping the vehicle or detaining the occupants of a parked or stopped vehicle. Do not simply assume that another officer has done so.

In the event the suspect vehicle or an occupant commits a violation of the law then the vehicle can be stopped or the occupants detained as in any other such incident.

462.4 DATA COLLECTION AND RETENTION

The Support Services Assistant Chief is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

Adoption Date: 2016/03/24

The Records Manager is responsible to ensure proper collection and retention of ALPR data, and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

Collection and retention of ALPR data is subject to the following guidelines:

(a) Files will be transferred from field units to department servers in accordance with the Alhambra Police Department file storage procedures.

(b) All ALPR data captured during a shift should be transferred to the department server before the end of each shift.

(c) All ALPR data is temporarily stored on the ALPR computer, separate from the MDC, before uploading to the server where the data is permanently stored.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged 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. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

462.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Alhambra 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 non-law enforcement requests for access to stored ALPR data shall be referred to theRecords Manager and processed in accordance with applicable law.

(b) 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).

(c) 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.

(d) ALPR system audits should be conducted on a regular basis. The Records Manager willprovide a monthly audit report of the ALPR usage, records sharing, and hotlists entries.

(e) Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected. Officers shall not attempt to modify or change the ALPR equipment or software unless authorized to do so by a supervisor.

(f) All successful uses of the ALPR shall be documented and forwarded to the Field Services Assistant Chief or his/her designee. The Field Services Assistant Chief or their designee will compile statistics of these uses and provide monthly updates on such uses to the Department’s command staff.

Adoption Date: 2016/03/24

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

462.6 POLICY

The policy of the Alhambra 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.

462.7 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 Support Services Assistant Chief 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).

462.8 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).

Adoption Date: 2016/03/24

Records Maintenance and Release

810.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

810.2 POLICY

The Alhambra Police Department is committed to providing public access to records in a manner that is consistent with the California Public Records Act (Government Code § 6250 et seq.).

810.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Records Manager or his/her designee, is normally the custodian of records for the Department, but the ultimate responsibility lies with the Support Services Division Commander. The responsibilities of the Custodian of Records include, but are not limited to:

(a) Managing the records management system for the Department, including the retention, archiving, release and destruction of department public records.

(b) Maintaining and updating the department records retention schedule including:

1. Identifying the minimum length of time the Department must keep records.
2. Identifying the department division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of department public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring a current schedule of fees for public records as allowed by law is available (Government Code § 6253).

(g) Ensuring that public records posted on the Department website meet the requirements of Government Code § 6253.10 including, but not limited to, posting in an open format where a record may be retrieved, downloaded, indexed and searched by a commonly used Internet search application.

(h) Ensuring that a list and description, when applicable, of enterprise systems (as defined by Government Code § 6270.5) is publicly available upon request and posted in a prominent location on the Department's website.

810.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for records shall route the request to the Custodian of Records or the authorized designee.

Adoption Date: 2016/03/24

810.4.1 REQUESTS FOR RECORDS

Any member of the public, including the media and elected officials, may access unrestricted records of this department, during regular business hours by submitting a written and signed request that reasonably describes each record sought and paying any associated fees (Government Code § 6253).

The processing of requests for records is subject to the following (Government Code § 6253):

(a) The Department is not required to create records that do not exist.

(b) Victims of an incident or their authorized representative shall not be required to show proof of legal presence in the United States to obtain department records or information. If identification is required, a current driver's license or identification card issued by any state in the United States, a current passport issued by the United States or a foreign government with which the United States has a diplomatic relationship or current Matricula Consular card is acceptable (Government Code § 6254.30).

(c) Either the requested record or the reason for non-disclosure will be provided promptly, but no later than 10 days from the date of request, unless unusual circumstances preclude doing so. If more time is needed, an extension of up to 14 additional days may be authorized by the Custodian of Records or the authorized designee. If an extension is authorized, the Department shall provide the requester written notice that includes the reason for the extension and the anticipated date of the response.

    1. When the request does not reasonably describe the records sought, the Custodian of Records shall assist the requester in making the request focused and effective in a way to identify the records or information that would be responsive to the request including providing assistance for overcoming any practical basis for denying access to the records or information. The Custodian of Records shall also assist in describing the information technology and physical location in which the record exists (Government Code § 6253.1).

(d) Upon request, a record shall be provided in an electronic format utilized by the Department. Records shall not be provided only in electronic format unless specifically requested (Government Code § 6253.9).

(e) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

    1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions.

(f) If a record request is denied in whole or part, the requester shall be provided a written response that includes the statutory exemption for withholding the record or facts that the public interest served by nondisclosure outweighs the interest served by disclosure (Government Code § 6255). The written response shall also include the names, titles or positions of each person responsible for the denial.

810.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record or any department record, including traffic collision reports, are restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Social Security numbers (Government Code § 6254.29).

(c) Personnel records, medical records and similar records which would involve an unwarranted invasion of personal privacy (Government Code § 6254; Penal Code § 832.7; Penal Code § 832.8; Evidence Code § 1043 et seq.).

1. Peace officer personnel records are deemed confidential and shall not be made public or otherwise released to unauthorized individuals or entities absent a valid court order.

2. The identity of any officer subject to any criminal or administrative investigation shall not be released without the consent of the involved officer, prior approval of the Chief of Police or as required by law.

(d) Victim information that may be protected by statutes, including victims of certain crimes who have requested that their identifying information be kept confidential, victims who are minors and victims of certain offenses (e.g., sex crimes, Penal Code § 293). Addresses and telephone numbers of a victim or a witness to any arrested person or to any person who may be a defendant in a criminal action shall not be disclosed, unless it is required by law (Government Code § 6254; Penal Code § 841.5).

1. Victims of domestic violence or their representative shall be provided, without charge, one copy of all domestic violence incident report face sheets, one copy of all domestic violence incident reports, or both, pursuant to the requirements and time frames of Family Code § 6228.

(e) Information involving confidential informants, intelligence information, information that would endanger the safety of any person involved or information that would endanger the successful completion of the investigation or a related investigation. This includes analysis and conclusions of investigating officers (Evidence Code § 1041; Government Code § 6254).

1. Absent a statutory exemption to the contrary or other lawful reason to deem information from reports confidential, information from unrestricted agency reports shall be made public as outlined in Government Code § 6254(f).

(f) Local criminal history information including, but not limited to, arrest history and disposition, and fingerprints shall only be subject to release to those agencies and individuals set forth in Penal Code § 13300.

1. All requests from criminal defendants and their authorized representatives (including attorneys) shall be referred to the District Attorney, City Attorney or the courts pursuant to Penal Code § 1054.5.

(g) Certain types of reports involving, but not limited to, child abuse and molestation (Penal Code § 11167.5), elder and dependent abuse (Welfare and Institutions Code § 15633) and juveniles (Welfare and Institutions Code § 827).

(h) Sealed autopsy and private medical information concerning a murdered child with the exceptions that allow dissemination of those reports to law enforcement agents, prosecutors, defendants or civil litigants under state and federal discovery laws (Code of Civil Procedure §130).

(i) Information contained in CCW permit applications or other files which would tend to reveal where the applicant is vulnerable or which contains medical or psychological information (Government Code § 6254).

(j) Traffic collision reports (and related supplemental reports) shall be considered confidential and subject to release only to the California Highway Patrol, Department of Motor Vehicles (DMV), other law enforcement agencies and those individuals and their authorized representatives set forth in Vehicle Code § 20012.

(k) Any record created exclusively in anticipation of potential litigation involving this department (Government Code § 6254).

(l) Any memorandum from legal counsel until the pending litigation has been adjudicated or otherwise settled (Government Code § 6254.25).

(m) Records relating to the security of the department's electronic technology systems (Government Code § 6254.19).

(n) Any other record not addressed in this policy shall not be subject to release where such record is exempt or prohibited from disclosure pursuant to state or federal law, including, but not limited to, provisions of the Evidence Code relating to privilege (Government Code § 6254).

(o) Information connected with juvenile court proceedings or the detention or custody of a juvenile. Federal officials may be required to obtain a court order to obtain certain juvenile information (Welfare and Institutions Code § 827.9; Welfare and Institutions Code § 831).

(p) The City Attorney is the ultimate authority when deciding whether police records shall be released.

810.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, City Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

Adoption Date: 2016/03/24

810.7 RELEASED RECORDS TO BE MARKED

Each page of any record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

810.8 SEALING OF CRIMINAL RECORDS

The Police Department will seal criminal records upon court ordered sealing. All record's sealing so ordered shall become the responsibility of the Records Section Manager or his/her designee.

Upon receipt of a bonafide court order to seal a criminal record, the records manager or his/her designee shall:

(a) Complete the compliance section of the court order.

(b) Mail a copy of the court order with a letter acknowledging completion of sealing to the Department of Justice, CII.

(c) Mail the disposition letter to the court that has ordered the sealing.

810.9 EXPUNGEMENT

Expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall expunge such records as ordered by the court. Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once the record is expunged, members shall respond to any inquiry as though the record did not exist.

810.10 SECURITY BREACHES

The Records Manager shall ensure notice is given anytime there is a reasonable belief an unauthorized person has acquired unencrypted personal identifying information stored in any Department information system (Civil Code § 1798.29).

Notice shall be given as soon as reasonably practicable to all individuals whose information may have been acquired. The notification may be delayed if the Department determines that notification will impede a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

For the purposes of this requirement, personal identifying information includes an individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number
- Driver license number or California identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Medical information
- Health insurance information

Adoption Date: 2016/03/24

- A username or email address, in combination with a password or security question and answer that permits access to an online account
- Information or data collected by Automated License Plate Reader (ALPR) technology

810.10.1 FORM OF NOTICE

(a) The notice shall be written in plain language, be consistent with the format provided in Civil Code § 1798.29 and include, to the extent possible, the following:

1. The date of the notice.
2. Name and contact information for the Alhambra Police Department.
3. A list of the types of personal information that were or are reasonably believed to have been acquired.
4. The estimated date or date range within which the security breach occurred.
5. Whether the notification was delayed as a result of a law enforcement investigation.
6. A general description of the security breach.
7. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a Social Security number or a driver license or California identification card number.

(b) The notice may also include information about what the Alhambra Police Department has done to protect individuals whose information has been breached and may include information on steps that the person whose information has been breached may take to protect him/herself (Civil Code § 1798.29).

(c) When a breach involves an online account, and only a username or email address in combination with either a password or security question and answer that would permit access to an online account, and no other personal information has been breached (Civil Code § 1798.29):

1. Notification may be provided electronically or in another form directing the person to promptly change either his/her password or security question and answer, as applicable, or to take other appropriate steps to protect the online account with the Department in addition to any other online accounts for which the person uses the same username or email address and password or security question and answer.
2. When the breach involves an email address that was furnished by the Alhambra Police Department, notification of the breach should not be sent to that email address but should instead be made by another appropriate medium as prescribed by Civil Code § 1798.29.

810.10.2 MANNER OF NOTICE

(a) Notice may be provided by one of the following methods (Civil Code § 1798.29):

1. Written notice.
2. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001.

3. Substitute notice if the cost of providing notice would exceed $250,000, the number of individuals exceeds 500,000 or the Department does not have sufficient contact information. Substitute notice shall consist of all of the following:
    (a) Email notice when the Department has an email address for the subject person.
    (b) Conspicuous posting of the notice on the department's webpage for a minimum of 30 days.
4. Notification to major statewide media and the California Information Security Office within the California Department of Technology.

(b) If a single breach requires the Department to notify more than 500 California residents, the Department shall electronically submit a sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

ALHAMBRA POLICE DEPARTMENT Date:	
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information.	
For More Information.	Call (626) 570-5151 or go to www.cityofalhambra.org/page/22/police_department/