DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX
Coordinator: Information Technology Unit

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the 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 contains investigatory and/or confidential information, it is not open to public review.

A. Description of the Technology

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images.

A – 1. How ALPR Works

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database. This process allows for two functions by ALPR:

1. Immediate (real time) comparison of the license plate characters against specific databases such as those provided by the California Department of Justice listing vehicles that are stolen or sought in connection with a crime or missing persons.
2. Storage of the license plate characters – along with the date, time, and location where the photography was taken ~~of the license plate~~ – in a ~~forward-facing graphical user interface~~ database that is accessible by law enforcement agencies for investigative query purposes.

A – 2. The ALPR System

There are two components to the ALPR system:

1. Automated License Plate Readers: These devices include cameras which can be attached to vehicles or fixed objects and a computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hotlists; data is transmitted for comparison (the hotlists are downloaded to the vehicle at the start of the

patrol shift and then compared from that list)~~, and a corresponding device that transmits collected data to various state databases for comparison and a central repository for storage and later retrieval~~.

2. ALPR Database: A~~This~~ central repository stores data collected and transmitted by the Automated License Plate Readers.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians or other OPD authorized ~~, OPD parking~~ personnel may ~~are authorized to~~ use the technology. Other authorized users may be designated by the Chief of Police or designee.

B – 2. Restrictions on Use

1. 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); authorized purposes consist only of queries related to criminal investigations, administrative investigations, and other authorized law enforcement functions, at the approval of a commander at rank of Deputy Chief or Deputy Director.

2. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

3. No ALPR operator may access department, state or federal data unless otherwise authorized to do so pursuant to Section D1 below.

4. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.

C. ALPR Data

C – 1. Data Collection and Retention

1. Transfer of Data

   Data will be transferred from vehicles to the designated storage in accordance as defined and designed by the ALPR technology system provider data transfer protocol.

2. Data Retention

All ALPR data downloaded to the server shall be purged in the server at the point of ~~730~~ 365 days in the server system. Data may be retained outside the database for the following purposes:

a. A criminal investigation;
b. An administrative investigation;
c. Research;
d. Civil litigation;
e. Training; and/or
f. Other Departmental need – with written authority from the Deputy Chief or Deputy Director.

C – 2. Data Security

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

1. All ALPR server data 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).

2. Members approved to access ALPR data under these guidelines are permitted to access the data for ~~legitimate~~ law enforcement purposes only.

3. ALPR system audits shall be conducted on a regular basis by the Bureau of Services to ensure proper system functionality; designated personnel will notify the City's Privacy Advisory Commission (PAC) in the event that the ALPR system cannot fully produce system audits due to technical issues with the system, and collaborate with the PAC to develop a plan to ensure audit functionality.

C – 3. Releasing or Sharing ALPR Server Data

ALPR server 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~~:

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-9.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

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

D. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Bureau of Services.

D – 1. ALPR Administrator

The Bureau of Services Deputy Chief or Deputy Director shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The Bureau of Services Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

D – 2. ALPR Coordinator

The title of the official custodian of the ALPR system is the ALPR Coordinator.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of ALPR technology to ensure the proper functionality of the system.

The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report in accordance with the requirements of OMC 9.64 (Oakland Surveillance Technology Ordinance).

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

By Order of

Susan E. Manheimer
Chief of Police Date Signed: