THE CITY OF BRENTWOOD

POLICE DEPARTMENT

Draft: March 23, 2016

AUTOMATED LICENSE PLATE READERS (ALPR) POLICY

I. PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology provides automated detection of license plates. The ALPR system captures an infrared image of a license plate and converts it to a text file using optical character recognition technology. The Brentwood Police Department (Department) uses ALPRs and supporting software to enable the rapid identification and location of vehicles of legitimate interest to law enforcement. ALPR units are placed at fixed locations, in officer vehicles, and in a portable trailer in the City where they collect license plate information from vehicles on public roadways and public property.

The license plate information is compared against law enforcement lists ("hotlists") of vehicles associated with active investigations, for example stolen vehicles, stolen license plates, Amber Alerts or other missing children. The system generates an alert when there is a hit, or match.

This Policy defines the minimum set of binding guidelines governing the collection and use of ALPR data in a manner consistent with respect for individuals' privacy and civil liberties.

II. ADMINISTRATION

The Police Department Patrol Captain or his or her designee will manage the installation and maintenance of ALPR equipment, as well as the ALPR data retention and access. The Captain will ensure that the ALPR system is operated in conformance with this Policy. The Captain may assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

III. ALPR OPERATION

A. Authorized locations and uses.

ALPR units may only be used to collect data that is within public view. The ALPR cameras may be installed at fixed locations in the City as determined by the Department.

Department sworn officers with a need and right to know will use ALPR technology to:

1. Locate stolen, wanted, and subject-of-investigation vehicles;

2. Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;

3. Locate witnesses and victims of violent crime;

4. Locate missing children and elderly individuals, including responding to Amber and Silver Alerts;

5. Support local, state, and federal public safety departments in the identification of vehicles associated with targets of criminal investigations; and

6. Protect critical infrastructure sites.

B. Verification before taking action. No action may be taken solely on an ALPR alert. Officers must verify an ALPR response through the California Law Enforcement Telecommunication System (CLETS) before taking law enforcement action.

Despite ongoing efforts to keep data current, the hotlists may or may not be accurate. Officers must separately verify the vehicle and subject information, and justification for contact. Officers must also visually confirm the plate characteristics generated by the ALPR reader.

C. Prohibited uses. No person may use the ALPR system for any of the following uses. Violation may result in criminal prosecution, civil liability, and/or administrative investigation pursuant to the Department Policy Manual.

1. Invasion of privacy. No person may use the ALPR system to record license plates except those license plates that are exposed to public view, or under a court order.

2. Harassment or intimidation. No person may use the ALPR system to harass and/or intimidate an individual or group.

3. Personal use. No person may use the ALPR system or associated files or hot lists for any personal purpose.

IV. RESTRICTIONS ON DATA COLLECTION; RETENTION

A. Restrictions on data collection. All data and images gathered by an ALPR unit are for the official use of the Department. Because the data may contain confidential CLETS information, and involves individuals' privacy, it is not open to public review. ALPR information gathered and retained by the Department may be used and shared with prosecutors or others only as permitted by law. (Gov't. Code §§6254(f) and (k).)

ALPR information is restricted to legitimate law enforcement uses, to further legitimate law enforcement goals and to enhance public safety. ALPR information may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States or California Constitutions.

B. Retention. ALPR data downloaded to the applicable server (under contract with the City) must be stored for a minimum of one year. (Government Code §34090.6) After that it will be destroyed unless it has become or is likely to become evidence in a criminal or civil action, or is subject to a lawful action to produce records. In those circumstances, only the applicable data should be downloaded from the server onto portable media and booked into evidence.

V. ACCOUNTABILITY AND SAFEGUARDS

The Department will closely safeguard and protect the saved ALPR data by both procedural and technological means. The Department will observe the following safeguards regarding access to and use of stored data:

1. Any non-law enforcement request for access to stored ALPR data must be referred to the Captain and processed in accordance with applicable law.

2. ALPR data will be stored in a secured law enforcement or contractor's facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff in good standing who have completed background investigations.

3. Any ALPR data downloaded to storage servers will be accessible only through strong multi-factor authentication and protected by encrypted communications, firewalls and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

4. Persons approved to access ALPR data under this Policy 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 investigation. To ensure proper operation and facilitate oversight, all users will be required to have individual credentials for access and use of the ALPR system.

CJIS[1]-compliant passwords and password change policies will be used together with two-factor authentication. Users who have been inactive for a period of time will be automatically disabled, requiring the re-activation by a system manager.

5. The ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes. The Chief

[1] Criminal Justice Investigation Services, a division of the FBI.

of Police may enter into service agreements with other law enforcement agencies to receive, provide, or share ALPR services that meet the minimum standards of this Policy.

6. ALPR system audits must be conducted on a periodic basis by the Captain.

7. Except as required by law, the ALPR system data may not be released, sold to, or exchanged for any commercial purpose, or to private entities or individuals.

8. The City and any contractor providing ALPR data to the City are subject to Civil Code sections 1798.29 and 1798.82 (SB 34) regarding security breaches involving personal information.

VI. TRAINING

Only persons trained in the use of the ALPR system within the prior year, including its privacy and civil liberties protections, is allowed access to the ALPR data. Training will consist of:

1. Legal authorities, developments, and issues involving the use of ALPR data and technology;

2. Current policy regarding appropriate use of ALPR systems;

3. Evolution of ALPR and related technologies, including new capabilities and associated risks;

4. Technical, physical, administrative, and procedural measure to protect the security of ALPR data against unauthorized access or use;

5. Practical exercises in the use of the current ALPR system.

Training will be updated as technological, legal, and other changes that affect the use of the ALPR system occur.

Approved by _____, Mark Evenson, Chief of Police

Dated: _____