STATE OF DELAWARE
DEPARTMENT OF SAFETY AND HOMELAND SECURITY
DIVISION OF STATE POLICE
P.O. BOX 430
DOVER, DELAWARE 19903

June 3, 2015

Jonathan Rudenberg
MuckRock News

Dear Mr. Rudenberg:

By email you requested "All documents relating to usage of Automated License Plate Recognition (ALPR) technology by the Delaware Department of Transportation, including but not limited to documents indicating:

- Scope of ALPR deployment;
- Purposes for which ALPR technology is employed;
- Means of handling and storing ALPR data
- Extent and timeline for ALPR data storage; and
- Protocols and extent of ALPR data sharing between DelDOT and other government agencies."

The Delaware State Police Automated License Plate Reader Policy is attached.

Sincerely,

Col. Nathaniel McQueen

Colonel Nathaniel McQueen, Jr.
Superintendent

AUTOMATED LICENSE PLATE READER POLICY

Purpose

The purpose of this policy is to establish guidelines for the use of Automated License Plate Readers (ALPR) by Delaware State Police personnel.

Definitions

A. Hot List: All data entered into the hot list download (stolen plates, stolen vehicles, uninsured motorist info, etc.) via NCIC/DELJIS. Also referred to as "Target List"

B. Hot List Download: The method, by which, the hot list data is transferred to the vehicle computer.

C. Authorized User: Any member of the division approved by the Superintendent, Executive Staff, or their designee that has been trained in the use of the ALPR.

Overview

The ALPR uses specialized cameras and computers to quickly capture large numbers of license plate photographs and compares them to a list of plates of interest. The plates of interest are referred to as a "hot list." The Executive Staff shall determine the primary groups of vehicles or tags of interest (e.g. Identification of stolen vehicles or license plates, uninsured motorists, wanted or missing person, and/or active criminal investigations.) ALPR systems can identify a target plate within seconds of contact, allowing law enforcement to identify target vehicles that may otherwise be overlooked. ALPR systems record license plates they come in contact with recording the location, date, and time of each license plate read. The technology is available in both mobile systems mounted on police vehicles and fixed camera systems mounted on poles or on the roadside. Mobile ALPR systems are designed to allow officers to patrol at normal speeds while the system reads license plates within system range and alerts if there is a match to a pre-defined "hot or target list."

Policy added: September 2010
OPR: Traffic

Deployment

The mobile ALPR unit consists of one or more cameras which are normally mounted on brackets on the trunk of a patrol vehicle. Other vehicle mounting configurations may be used based on the availability of resources and the nature of the investigation. The Director of Information Technology will establish all deployment protocols. The ALPR cameras can be aimed to read license plates of vehicles ahead, on either side, or traveling in the opposite direction of the patrol vehicle. The images captured by the cameras are displayed on the in-car Mobile Data Computer (MDT), where they are automatically searched against the hot list data base. When a target plate is identified, an alert message and audible tone are displayed on the MDT.

Alerts, Verification, and Enforcement

An alert of the ALPR is a preliminary notification of a possible hit from the targeted list of vehicles. An alert received by the ALPR is **NOT** deemed probable cause to conduct a traffic stop. This does not preclude an authorized user from engaging in enforcement action if other probable cause exists. Authorized users acting solely on an ALPR alert are not to take any enforcement action until additional verifications take place.

These additional steps will include at a minimum:

- Visual verification that the license plate number and state match exactly
- Verify the status of the plate and/or vehicle in the NCIC and/or DELJIS databases

Hot List or Target List

The hot list database is updated daily and the hot list download is performed via a wireless data transmission function. The authorized user of the ALPR is not required to perform any type of manual download to have the most current and updated hot list. The Director of Information Technology will be responsible for establishing daily system updating.

The ALPR database can be amended by the authorized user at any time, by inputting the necessary information directly into the MDT application. This type of updating will allow the ALPR to scan for plates which were not in the database at the start of the shift, such as Amber Alert, BOLOs, or tags of interest received during the shift. It is important to note that if an entry is manually inputted into the system, that only the users system will scan for the tag information. The manually inputted information is not shared or transmitted to other ALPR user systems. Authorized users shall only input license plate data that is part of a bona fide investigation or already identified in the target list.

Authorized users inputting their own tag data will be required to provide electronic justification for each entry. These entries will be electronically tracked and archived for a minimum period of one year.

Data Retention, Access, and Dissemination

Data will be stored and managed by the Director of Information Technology. Security, access, retention, archiving, and purging will be in accordance with this policy and standard operating procedures set forth by the Director of Information Technology as approved by the Executive Staff.

Retention

Data will be temporarily stored and available on the authorized user's MDT. Information Technology will automatically download and purge the data from the MDT on a schedule set forth by Information Technology based on system operational parameters. This frequency of the download and purging of data on the MDT should not exceed ten (10) days. During the temporary retention period, the authorized user may review hits or alerts registered by their MDT. Review or search of other data temporarily retained on the MDT will require electronic verification of the reason for the search (i.e. Robbery, in progress crime) Any data obtained may be disseminated in accordance to this policy. All inquiries will be electronically logged and archived for no less than one (1) year.

Data that is downloaded from mobile units will be actively retained in a database maintained and secured by Information Technology for a period of one year. After a period of one year, data will then be retained in an archive database for up to five (5) years depending on system storage capacity.

Access

Any authorized member of the Delaware State Police conducting an active investigation may have access to the retained data. Authorized members will be required to verify their identity and purpose of the inquiry according to system protocols. The Director of Information Technology shall establish protocols to ensure that all database inquiries are recorded and archived for a period of no less than one (1) year.

Normal inquiries will only search the active year database. Inquiries greater than one year will require approval from a commissioned officer and be made to the Director of Information Technology or their designee. Each separate investigation shall require special authorization. The Director of Information Technology, upon receiving proper authorization, shall permit access to archived data according to system protocols.

All results of inquiries are to be documented by the investigator in the incident report.

Authorized users shall not disseminate information from ALPR mobile units, or the databases, outside the Delaware State Police.

Images and/or data that may be of evidentiary value may be downloaded to a media approved by Information Technology and retained by the investigator until the investigation is fully adjudicated. After the case has been adjudicated the media containing ALPR downloaded data or images will be disposed of in accordance to divisional policy.

Access requests from outside agencies

All requests are to be in writing (or electronic e-mail) to the Director of Information Technology, or designee, and be authorized by a commissioned officer of the requesting agency. The request must contain an incident complaint number and the recipient of the information must agree that the data will not be disseminated outside their agency. The Director of Information Technology shall maintain a log, either written or electronic, of all inquiries.

> ***Exigent circumstances:*** In the event of an exigent circumstance (e.g. Robbery, Homicide, Abduction, Amber Alert etc) Trooper's may access data retained on their respective MDT with the approval of the on-duty supervisor. All inquiries for other agencies will be documented in an "Assist Other Agency" paper report (Not a Field Service Report). This report will document the exigent circumstance, name of approving supervisor, and the complaint number of the requesting agency.

Audit

The Director of Information Technology shall conduct an audit annually to ensure that archiving and purging requirements have been met. In addition, the Director shall, at least bi-annually, randomly audit inquiries made by authorized members of the division to ensure compliance with this policy.

Training

Only trained authorized members of the division shall operate the ALPR systems. Training requirements shall be established by the Director of Information Technology.

Maintenance

Mobile ALPR systems will be installed in vehicles as determined by the Operations Major or his designee. Information Technology will be responsible for the installation and maintenance of the server, mobile computer systems, and related software. Any damage to the ALPR system should be reported immediately according to established divisional policy. ALPR equipment should be cleaned and maintained according to the manufacturer's recommendations. At the conclusion of the users shift, the camera's are to be removed and stored in the cases that are provided with the unit. This would also apply, if the unit will not be in operation for an extended period of time during the users shift (court, processing and arraigning prisoners, etc). It is imperative that the unit be turned off prior to any camera removal or internal maintenance to the unit.