

**FLORIO & KENNY, L.L.P.**

ATTORNEYS AT LAW

5 MARINE VIEW PLAZA  
SUITE 103  
P.O. BOX 771  
HOBOKEN, NEW JERSEY 07030  
PHONE: (201) 659-8011  
FAX: (201) 659-8511/0884

E-MAIL: [MAIN@FLORIOKENNYLAW.COM](mailto:MAIN@FLORIOKENNYLAW.COM)WEBSITE: [WWW.FLORIOKENNYLAW.COM](http://WWW.FLORIOKENNYLAW.COM)

EDWARD J. FLORIO  
BERNARD F. KENNY, JR.  
NITI G. RAVAL

CHRISTOPHER L. PATELLA  
OF COUNSEL

CHRISTOPHER K. HARRIOTT  
DAVID J. YANOTCHKO  
DENNIS P. LILOIA  
STEPHEN R. BANKS^  
MICHELE C. SEBASTIANO\*  
MELISSA B. PAOLELLA\*  
MICHAEL T. WILKOS\*

^ CERTIFIED WORKER'S  
COMPENSATION ATTORNEY

\* ADMITTED TO NJ & NY BAR

September 28, 2012

**VIA FACSIMILE (973-642-6523)**

Thomas W. MacLeod, Esq.  
Open Governance Attorney  
American Civil Liberties Union of New Jersey  
P.O. Box 32159  
Newark, New Jersey 07102

Re: OPRA Request for ALPR documents  
Our File No. 5004.001

Dear Mr. MacLeod:

Please be advised that this firm serves as City Attorney for the City of Passaic. Please accept this letter in furtherance of my previous correspondence regarding your July 30, 2012 OPRA request served on the City of Passaic seeking numerous documents related to Automatic License Plate Recognition ("ALPR") technology.

Specifically, your request sought the following records from 2006 to present:

1. Policies, procedures and general guidelines pertaining to ALPR technology;
2. Procurement of ALPR technology;
3. Use of APLR technology

**17714**

4. Storage of data scanned with ALPR technology;
5. Accessing ALPR data;
6. Sharing ALPR data; and
7. Training materials used in the instruction of ALPR technology.

The City of Passaic hereby responds as follows:

1. See attached Attorney General Directive No. 2010-5.
2. The City of Passaic is not in possession of any records responsive to this request.
3. Denied. These records are exempt from production as a criminal investigatory record pursuant to N.J.S.A. 47:1A-1 and Attorney General Directive No. 2010-5. These records are also exempt from production as they are "records related to security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software" pursuant to N.J.S.A. 47:1A-1. These records are also exempt as they are "administrative or technical information regarding computer hardware, software and networks which, if disclosed would jeopardize computer security." Finally, pursuant to N.J.A.C. 13:1E-3.2(a)(1), these records are exempt from disclosure as they relate to "standard operating procedures and training materials that would reveal agency investigative, enforcement or litigation procedures or techniques."
4. Denied. These records are exempt from production as a criminal investigatory record pursuant to N.J.S.A. 47:1A-1 and Attorney General Directive No. 2010-5. These records are also exempt from production as they are "records related to security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software" pursuant to N.J.S.A. 47:1A-1. These records are also exempt as they are "administrative or technical information regarding computer hardware, software and networks which, if disclosed would jeopardize computer security." Finally, pursuant to N.J.A.C. 13:1E-3.2(a)(1), these records are exempt from disclosure as they relate to "standard operating procedures and training materials that would reveal agency investigative, enforcement or litigation procedures or techniques."

**17715**

5. Denied. These records are exempt from production as a

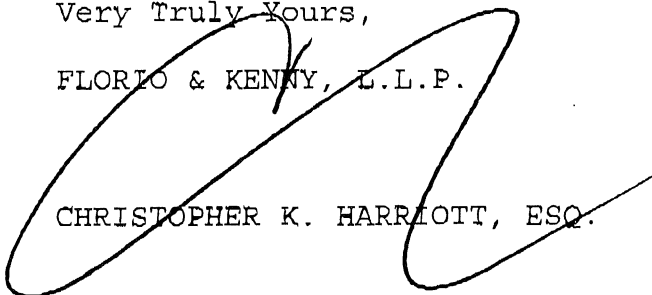
criminal investigatory record pursuant to N.J.S.A. 47:1A-1 and Attorney General Directive No. 2010-5. These records are also exempt from production as they are "records related to security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software" pursuant to N.J.S.A. 47:1A-1. These records are also exempt as they are "administrative or technical information regarding computer hardware, software and networks which, if disclosed would jeopardize computer security." Finally, pursuant to N.J.A.C. 13:1E-3.2(a)(1), these records are exempt from disclosure as they relate to "standard operating procedures and training materials that would reveal agency investigative, enforcement or litigation procedures or techniques."

6. Denied. These records are exempt from production as a criminal investigatory record pursuant to N.J.S.A. 47:1A-1 and Attorney General Directive No. 2010-5. These records are also exempt from production as they are "records related to security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software" pursuant to N.J.S.A. 47:1A-1. These records are also exempt as they are "administrative or technical information regarding computer hardware, software and networks which, if disclosed would jeopardize computer security." Finally, pursuant to N.J.A.C. 13:1E-3.2(a)(1), these records are exempt from disclosure as they relate to "standard operating procedures and training materials that would reveal agency investigative, enforcement or litigation procedures or techniques."
7. Denied. These records are exempt from production as a criminal investigatory record pursuant to N.J.S.A. 47:1A-1 and Attorney General Directive No. 2010-5. These records are also exempt from production as they are "records related to security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software" pursuant to N.J.S.A. 47:1A-1. These records are also exempt as they are "administrative or technical information regarding computer hardware, software and networks which, if disclosed would jeopardize computer security." Finally, pursuant to N.J.A.C. 13:1E-3.2(a)(1), these records are exempt from disclosure as they relate to "standard operating procedures and training materials that would reveal agency investigative, enforcement or litigation procedures or techniques."

Thank you for your attention to this matter. Please do not hesitate to contact the undersigned should you have any further questions.

Very Truly Yours,

FLORIO & KENNY, L.L.P.



CHRISTOPHER K. HARRIOTT, ESQ.

ENC.

CC: Amada Curling, City Clerk  
Deputy Chief Matthew Paz  
Christopher Hsieh, Passaic County Prosecutor's Office



CHRIS CHRISTIE  
Governor

KIM GUADAGNO  
Lieutenant Governor

*State of New Jersey*  
OFFICE OF THE ATTORNEY GENERAL  
DEPARTMENT OF LAW AND PUBLIC SAFETY  
PO BOX 080  
TRENTON, NJ 08625-0080

PAULA T. DOW  
Attorney General

**DIRECTIVE NO. 2010-5**

**TO:** Director, Office of Homeland Security and Preparedness  
Director, Division of Criminal Justice  
Superintendent, New Jersey State Police  
All County Prosecutors  
All County Sheriffs  
All Police Chiefs  
All Law Enforcement Chief Executives

**FROM:** Paula T. Dow, Attorney General

**DATE:** December 3, 2010

**SUBJECT:** Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data

In order to fulfill the mission of protecting the public, the New Jersey law enforcement community must take full advantage of new crime-fighting technologies as they become available. Automated license plate readers (ALPRs) are now being used by a number of law enforcement agencies around the nation, and a number of police agencies in New Jersey have recently acquired these devices or are planning to do so in the near future. License plate recognition technology can be used to support a wide range of law enforcement operations and activities, including homeland security, criminal and terrorist suspect interdiction, revoked/suspended driver interdiction, stolen property recovery, stay-away order enforcement and, of course, the apprehension of individuals who are subject to an outstanding arrest warrant.

These devices enable police officers to recognize and take immediate action against vehicles and persons who are subject to an investigative detention or arrest based on a "Be on the Lookout" bulletin. The data collected by ALPRs can also provide solid investigative leads if, for example, a device happened to be scanning license plates near a crime scene, allowing police to locate potential suspects, witnesses, or victims by identifying vehicles that were in the vicinity at the time of the



offense. A careful analysis of stored ALPR data can also be used to detect suspicious activities that are consistent with the *modus operandi* of criminals. This new technology can in this way serve an especially important role in protecting our homeland from terrorist attack, as shown by the fact that many of the devices that are now or soon will be in operation in this State were purchased with homeland security grant monies.

While license plate recognition technology can help to protect public safety, the widespread deployment and use of ALPRs, and especially the collection and storage of data pertaining to individuals who are not reasonably believed to be involved in unlawful activity, raise legal and policy issues. Notably, the New Jersey Supreme Court has held that while police are permitted to "run the plates" of any vehicle they encounter while on patrol, and need not have a particularized reason before checking a vehicle's license plates against a government database, police in this State may not as a result of any such lookup be shown personal identifying information about a motorist unless there is a particularized basis for further police action. See *State v. Donis*, 157 N.J. 44 (1998). The Guidelines attached hereto are designed to protect the legitimate privacy interests of motorists by implementing the non-disclosure rule established in *Donis* and by adapting the *Donis* Court's rationale to the context and capabilities of ALPR technology.

Recognizing that our experience with this new and evolving technology is limited, and that we still have much to learn about how best to incorporate these devices into our arsenal of investigative techniques, it is appropriate for me as the State's chief law enforcement officer to issue uniform statewide guidelines to ensure that ALPRs are used only for *bona fide* law enforcement purposes, and that the data collected by these devices are used in accordance with substantive standards and procedural safeguards that appropriately balance the need for law enforcement agencies to prevent and respond to terrorism and other forms of crime against the legitimate privacy interests of persons operating motor vehicles on the roadways of this State.

THEREFORE, I, Paula Dow, Attorney General of the State of New Jersey, pursuant to the authority granted to me by the Constitution of the State of New Jersey and by the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 *et seq.*, and in consultation with the Director of the New Jersey Office of Homeland Security and Preparedness, hereby Direct the following:

1. Adoption of Guidelines

The "Attorney General Guidelines for the Use of Automated License Plate Readers and Stored ALPR Data" (dated December 3, 2010) attached to this Directive and incorporated by reference into this Directive are hereby adopted and shall be followed and enforced by all law enforcement agencies and officers operating under

the authority of the laws of the State of New Jersey.

2. Implementation

Every law enforcement agency operating under the authority of the laws of the State of New Jersey that possesses or uses one or more automated license plate readers shall, within 45 days of the issuance of this Directive, promulgate and enforce a rule, regulation, standard operating procedure, directive, or order, in a form as may be appropriate given the customs and practices of the agency, which shall comply with and implement the provisions of the attached Guidelines, and which shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's rule, regulation, standard operating procedure, directive, or order shall be subject to discipline. A law enforcement agency operating under the authority of the laws of the State of New Jersey that purchases an automated license plate reader on or after the effective date of this Directive shall not operate the device without having promulgated a rule, regulation, standing operating procedure, directive, or order in accordance with this section.

3. Scope

The provisions of this Directive and of the attached Guidelines pertaining to stored ALPR data apply to all law enforcement agencies operating under the authority of the laws of the State of New Jersey that access or use stored ALPR data, even if the agency does not own or operate an ALPR.

4. Questions and Controversies

All questions concerning the interpretation, implementation, or enforcement of this Directive, or of the attached Guidelines, shall be addressed to the Attorney General or his or her designee.

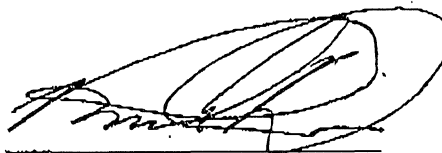
5. Periodic Review

The Director of the Division of Criminal Justice, in consultation with the Superintendent of the New Jersey State Police, the Director of the Office of Homeland Security, the County Prosecutors, the County Sheriffs, and the New Jersey Association of Chiefs of Police, shall, within one year of the effective date of this

Directive, report to the Attorney General on the implementation of this Directive, and on any recommendations for revising the attached Guidelines.

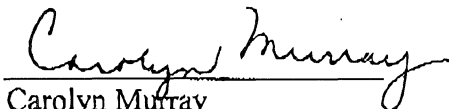
6. Effective Date

This Directive shall take effect 45 days after it is issued in order to provide an opportunity for law enforcement agencies to comply with its requirements and to establish and enforce policies and procedures consistent with the attached Guidelines. Once effective, this Directive shall remain in force and effect unless and until a repealed, amended, or superseded by Order of the Attorney General.



Paula T. Dow  
Attorney General

Attest:



Carolyn Murray  
Counsel to the Attorney General

Issued on: December 3, 2010  
Effective on : January 18, 2011



## ATTORNEY GENERAL GUIDELINES FOR THE USE OF AUTOMATED LICENSE PLATE READERS (ALPRs) AND STORED ALPR DATA

(Issued December 3, 2010; Effective January 18, 2011)

### 1. PURPOSE AND SCOPE

#### 1.1 Reasons for Promulgating Uniform Statewide Guidelines

The purpose of these Guidelines is to provide direction to law enforcement agencies and officers on the appropriate use of Automated License Plate Readers (ALPRs) and the data that are collected by these devices and stored for future law enforcement use. These Guidelines are not intended to serve as a comprehensive operational manual. Rather, they are meant to ensure that ALPRs and ALPR-generated data are used in an appropriate manner and only for *bona fide* public safety purposes.

The following Guidelines, which are promulgated pursuant to Attorney General Law Enforcement Directive 2010-5, should be interpreted and applied so as to achieve the following objectives:

- to ensure that "BOLO lists" (the compilation of targeted license plates that an ALPR is "on the lookout" for) that are programmed into the internal memory of an ALPR or that are compared against stored ALPR data are comprised only of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate, or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle's past location(s) through the analysis of stored ALPR data;
- to ensure that data that are captured by an ALPR can only be accessed by appropriate law enforcement personnel and can only be used for legitimate, specified, and documented law enforcement purposes;
- to permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst; and
- to ensure that stored ALPR data are purged after a reasonable period of time so as to

minimize the potential for misuse or accidental disclosure.

## 1.2 Applicability of Guidelines

These Guidelines apply to all law enforcement agencies that operate under the authority of the laws of the State of New Jersey that own or operate one or more ALPRs, that collect and maintain ALPR data, and/or that receive or are provided access to ALPR data collected by another agency.

## 1.3 Non-Enforceability of Rights by Third Parties

These Guidelines are issued pursuant to the Attorney General's authority under the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 et seq., to ensure the uniform and efficient enforcement of the laws. These Guidelines impose limitations on the exercise of law enforcement discretion and the use of and access to ALPR-related data that may extend beyond the requirements of the United States and New Jersey Constitutions, and federal and state statutory law. Nothing in these Guidelines should be construed in any way to create any rights beyond those established under the Constitutions, statutes, and regulations of the United States and the State of New Jersey. The provisions of these Guidelines are intended to be implemented and enforced by law enforcement agencies that possess or use ALPRs, the New Jersey Office of Homeland Security and Preparedness, the County Prosecutors, and the Department of Law and Public Safety, and these provisions do not create any rights that may be enforced by any other persons or entities.

## 3. **DEFINITIONS**

As used in these Guidelines:

"Automated License Plate Reader" or "ALPR" means a system consisting of a camera, or cameras, and related equipment that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device, that automatically converts digital photographic images of scanned license plates into electronic text documents, that is capable of comparing scanned license plate text data with data files for vehicles on a BOLO (be on the lookout) list programmed into the device's electronic memory, and that notifies police, whether by an audible alert or by other means, when a scanned license plate matches the license plate on the programmed BOLO list. The term includes both devices that are placed at a stationary location (whether permanently mounted, or portable devices positioned at a stationary location) and mobile devices affixed to a police vehicle and capable of operating while the vehicle is in motion.

"BOLO (Be on the Lookout)" or "BOLO situation" refers to a determination by a law

enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle, or, in the case of a post-scan BOLO, there is a legitimate and specific reason to ascertain the past location(s) of a particular vehicle.

"BOLO list," sometimes referred to colloquially as a "hot list," is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists that is programmed into an ALPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more license plates, or partial license plates, that is compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data that is stored in a separate data storage device or system.

"Initial BOLO list" refers to the BOLO list that was programmed into an ALPR at the time that the device was being used to scan license plates in the field.

"Post-Scan BOLO list" refers to a BOLO list that is compared against stored data collected by an ALPR, including scanned license plate data that has been transmitted to another device or data storage system.

"Stored data" refers to all information captured by an ALPR and stored in the device's memory or in a separate data storage device or system. The term includes the recorded image of a scanned license plate and optical character recognition data, a contextual photo (*i.e.*, a photo of the scanned vehicle and/or occupants), global positioning system ("GPS") data (when the ALPR is equipped with a GPS receiver) or other location information, and the date and time of the scan. The term applies to both alert data and non-alert data that has been captured and stored by an ALPR or in a separate data storage device or system.

"Alert data" means information captured by an ALPR relating to a license plate that matches the license plate on an initial BOLO list or a post-scan BOLO list.

"Immediate alert" refers to an alert that occurs when a scanned license plate matches the license plate on an initial BOLO list and that is reported to the officer operating the ALPR, by means of an audible alarm or by any other means, at or about the time that the subject vehicle was encountered by the ALPR and its license plate was scanned by the ALPR.

"Non-encounter alert" refers to an immediate alert where the officer operating the ALPR is instructed to notify the agency that put out the BOLO without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention (*e.g.*, a Violent Gang or Terrorist Organization File (VGTOF) alert).

"Personal identifying information" means information that identifies one or more specific individuals, including an individual's name, address, social security number, vehicle operator's

license number, or biometric records. The term includes personal identifying information that is included within the data comprising a BOLO list, as well as personal identifying information that is learned by checking a license plate scanned by an ALPR against the Motor Vehicle Commission database or any other data system that contains personal identifying information.

“Scan” refers to the process by which an ALPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the ALPR.

“Authorized user” means a sworn or civilian employee of a law enforcement agency who has been authorized by the chief of the agency, or by the Attorney General or a county prosecutor or his or her designee, to operate an ALPR, or to access and use ALPR stored data, and who has successfully completed training provided by the agency on the agency’s ALPR policy and on these Guidelines.

“Designated supervisor” means a superior officer assigned by the chief of a law enforcement agency to oversee and administer, or to assist in overseeing and administering, the agency’s use of ALPRs and stored ALPR data. A law enforcement agency may have more than one designated supervisor.

“Chief” of a department or agency means the highest ranking sworn officer of a law enforcement agency.

“Post-Scan BOLO query” refers to the process of comparing a post-scan BOLO list against stored ALPR data.

“Crime scene query” refers to the process of accessing and reviewing stored ALPR data that had been originally scanned at or about the time and in the vicinity of a reported criminal event for the purpose of identifying vehicles or persons that might be associated with that specific criminal event as suspects, witnesses, or victims.

“Criminal event” means a specific incident, or series of related specific incidents, that would constitute an indictable crime under the laws of the State of New Jersey, whether or not the incident(s) have occurred or will occur within the State of New Jersey. The term includes an attempt or conspiracy to commit a crime, or actions taken in preparation for the commission of the crime, such as conducting a surveillance of the location to identify and evade or thwart security measures, or conducting a rehearsal of a planned crime. The term includes two or more separate criminal acts or episodes that are linked by common participants or that are reasonably believed to have been undertaken by a criminal organization or as part of an ongoing conspiracy.

“Crime trend analysis” refers to the analytical process by which stored ALPR data is used, whether alone or in conjunction with other sources of information, to detect crime patterns by studying and linking common elements of recurring crimes; to predict when and where future crimes may occur; and to link specific vehicles to potential criminal or terrorist activity. The term includes

an automated process in which a computer program analyzes stored data to identify potentially suspicious activity or other anomalies involving one or more scanned vehicles and where such automated analysis is done without disclosing personal identifying information about any individual to an authorized user or any other person except as may be authorized pursuant to Section 10.2.3 of these Guidelines.

#### 4. DEPLOYMENT OF ALPRS

##### 4.1 Restricted Uses

An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business.

##### 4.2 ALPR Scanning Limited to Vehicles Exposed to Public View

An ALPR shall only be used to scan license plates 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 shopping mall or other business establishment).

##### 4.3 Supervisory Approval of All ALPR Deployments

An ALPR shall not be deployed in the field unless the deployment has been authorized by the chief of the department or a designated supervisor, or by the Attorney General or designee or a county prosecutor or designee. Such authorization may be given for repeated or continuous deployment of an ALPR (e.g., mounting the device on a particular police vehicle, or positioning the ALPR at a specific stationary location), in which event the deployment authorization shall remain in force and effect unless and until rescinded or modified by the chief or designated supervisor, or the Attorney General or county prosecutor or designee.

##### 4.4 Trained Operators and Analysts

A sworn officer or civilian employee of the department may operate an ALPR or access or use ALPR stored data only if the person has been designated as an authorized user by the chief of the department, or by the Attorney General or designee or a county prosecutor or designee, and has received training from the department on the proper use and operation of ALPRs, the requirements of Attorney General Law Enforcement Directive 2010-5, and these Guidelines, and any policies and

procedures governing the use of ALPRs and ALPR data issued by the department pursuant to Attorney General Directive 2010-5 and Section 14 of these Guidelines.

## 5. MAINTENANCE OF RECORDS

### 5.1 Records Documenting the Deployment of ALPRs

Each department that owns or operates an ALPR shall maintain a written or electronic record that documents the following information:

date and time when the ALPR was deployed;

whether the ALPR was mobile, or was stationed at a fixed specified location;

the identity of the operator;

whether ALPR data was transferred to any other database or data storage device or system.

### 5.2 Records Documenting the Use of Stored ALPR Data

Each department that stores ALPR data shall maintain a record of all access to stored ALPR data. The department's ALPR data record keeping system, which may be automated, shall document the following information:

the date and time of access, and, in the case of access to stored non-alert data, the type of access authorized by Section 10.2 of these Guidelines (*i.e.*, post-scan BOLO query, crime scene query, or crime trend analysis);

the authorized user who accessed the stored data;

whether an automated software program was used to analyze stored data;

the designated supervisor who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required by Section 10.2.3 of these Guidelines;

the designated supervisor who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying

information in accordance with Section 10.2.3;

any other information required to be documented pursuant to Section 10.2 or any other provision of these Guidelines.

### 5.3 Maintenance of Records

All written or electronic records of ALPR activity and access to ALPR data shall be maintained by the department for a period of five years, and shall be kept in a manner that makes such records readily accessible to any person authorized by these Guidelines to audit the department's use of ALPRs and ALPR-generated data. When a department employs an automated system to record any information that is required to be documented pursuant to these Guidelines, it shall not be necessary for the department to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.

## 6. **CONTENT AND APPROVAL OF BOLO LISTS**

### 6.1 Criteria for and Examples of Legitimate BOLO Situations

A license plate number or partial license plate number shall not be included in an ALPR initial BOLO list unless there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person or persons who are reasonably believed to be associated with that vehicle. A license plate or partial license plate number shall not be included in a Post-Scan BOLO list unless there is a legitimate and specific law enforcement reason to ascertain the past locations(s) of that particular vehicle, or of any person or persons who are reasonably believed to be associated with that vehicle.

Examples of legitimate and specific reasons include, but are not limited to: persons who are subject to an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are reasonably believed to be involved in the commission of a crime or disorderly persons offense; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list; vehicles with expired registrations or other Title 39 violations; persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and persons who are on any watch list issued by a State or federal agency responsible for homeland security.

## 6.2 Batch Downloading of BOLO List Data

BOLO list information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, United States Department of Homeland Security, and Motor Vehicle Commission database.

## 6.3 Updates to BOLO Lists

An initial BOLO list may be revised at any time. In the event that an initial BOLO list is constructed, in whole or in part, with sets of data downloaded from another database, so as to account for any changes that may have been made in the data maintained in those other databases, updates to the initial BOLO list shall, in the case of a mobile unit attached to a police vehicle, be made at the start of each shift, and in the case of an ALPR positioned at a stationary location, be made as frequently as is practicable, and on not less than a daily basis. Information concerning any license plate that is referenced in an AMBER Alert activated by the New Jersey State Police shall be added to the initial BOLO list as expeditiously as possible, and shall remain in the initial BOLO list until the AMBER Alert expires or is withdrawn.

## 6.4 Special Instructions for Immediate Alert Response

When practicable, the reason for placing a vehicle on BOLO list shall be included with the BOLO and shall be disclosed to the officer who will react to an immediate alert. If for any reason an officer reacting to an immediate alert should not initiate an investigative detention (*e.g.*, where the license plate was included in the BOLO list because the department or any other agency wanted to be notified of the location of the subject vehicle without alerting the driver/occupants that they are the subject of law enforcement attention, such as in the case of Violent Gang or Terrorist Organization File (VGTOF) alert), to the extent feasible, the information attached to the license plate on the BOLO list shall be entered in such a way as to cause the ALPR to clearly designate an immediate alert as a "non-encounter" alert, and shall provide specific instructions to the officer as to who to notify of the alert. See Section 7, *infra*.

## 7. **POLICE ACTIONS IN RESPONSE TO AN IMMEDIATE ALERT**

When an officer operating a vehicle equipped with an ALPR receives an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted to the fact that an observed motor vehicle's license plate is on the BOLO list may be required to make a reasonable effort to confirm that a wanted person is actually in the vehicle before



the officer would have a lawful basis to stop the vehicle. See State v. Parks, 288 N.J. Super. 407 (App. Div. 1996) (police do not have reasonable suspicion to justify a stop based on a computer check that shows that the operator's license of the registered owner of the vehicle is suspended unless the driver generally matches the owner's physical description (*e.g.*, age and gender)).

An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle had been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO. See Section 6.4, supra.

## **8. SECURITY OF STORED ALPR DATA**

### **8.1 Physical Security and Limited Access**

All ALPR stored data shall be kept in a secure data storage system with access restricted to authorized persons. Access to this stored data shall be limited to the purposes described in Section 10 of these Guidelines.

### **8.2 Differentiation of Stored Positive Alert Data From Non-Alert Data**

Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data so as to ensure that access to and use of non-alert data and any disclosure of personal identifying information resulting from the analysis of non-alert data occurs only as may be authorized pursuant to section 10.2 of these Guidelines. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file, see also Section 10.1, infra, and may as appropriate be placed into evidence in accordance with the department's evidence or records management procedures.

## **9. RETENTION PERIOD AND PURGING OF STORED DATA**

Each law enforcement agency shall, pursuant to the provisions of Section 14 of these Guidelines, establish and enforce procedures for the retention and purging of stored ALPR data in accordance with this Section. ALPR stored data shall be retained for a period of five years, after which, the data shall be purged from the agency's data storage device or system. A law enforcement agency may purge ALPR data before the expiration of the five-year retention period only if the data has been transferred to the State Police Regional Operations Intelligence Center (R.O.I.C.) or any other system that aggregates and stores data collected by two or more law enforcement agencies in accordance with the provisions of these Guidelines. Any ALPR data transferred to another agency

shall indicate the date on which the data had been collected by the ALPR so that the receiving agency may comply with the five-year retention and purging schedule established in this Section. See also Section 11.1 and 11.2, infra.

## 10. LIMITATIONS ON ACCESS TO AND USE OF STORED ALPR DATA

### 10.1 Access to Positive Alert Data

An authorized user may access and use stored ALPR alert data as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a post-scan BOLO query, a crime scene query, or crime trend analysis. A record shall be made of the access to the data, which may be an automated record, that documents the date of access, and the identity of the authorized user. An authorized user need not obtain approval from the chief or designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored ALPR data. Once positive alert data has been accessed and transferred to an investigation file, it shall not be necessary thereafter to document further access or use of that data pursuant to these Guidelines.

### 10.2 Access to Non-Alert Data

Access to and use of stored non-alert ALPR data is limited to the following three purposes: a post-scan BOLO query, a crime-scene query, and crime trend analysis. An authorized user does not need to obtain approval from the chief or a designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored non-alert data pursuant to this Section.

#### 10.2.1 Post-Scan BOLO Query

A law enforcement agency is authorized to compare a post-scan BOLO list against stored ALPR data where the results of the query might reasonably lead to the discovery of evidence or information relevant to any active investigation or ongoing law enforcement operation, or where the subject vehicle might be placed on an active initial BOLO list. (For example, a law enforcement agency may review stored non-alert data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned for the purpose of confirming or dispelling an alibi defense, or to develop lead information for the purpose of locating a specified vehicle or person. A law enforcement agency may also check stored data to determine whether a vehicle that was only recently added to an initial BOLO list had been previously observed in the jurisdiction before it had been placed on an initial BOLO list.)

### 10.2.2 Crime Scene Query

a. A law enforcement agency is authorized to access and use stored non-alert data where such access might reasonably lead to the discovery of evidence or information relevant to the investigation of a specific criminal event as defined in these Guidelines. Note that if the law enforcement agency has reason to believe that a specific person or vehicle was at or near the location of the specific crime at the time of its commission, non-alert stored data might also be examined under the authority of Section 10.2.1 as part of post-scan BOLO query.

b. A crime scene query may not be conducted to review stored non-alert data based on general crime patterns (*i.e.*, *e.g.*, to identify persons traveling in or around a "high crime area"), but rather is limited to situations involving specific criminal events as that term is defined in these Guidelines.

c. The crime scene query of non-alert stored data shall be limited in scope to stored non-alert data that is reasonably related to the specified criminal event, considering the date, time, location, and nature of the specified criminal event. For example, a crime that reasonably involves extensive planning and possible "rehearsals," such as a terrorist attack, would justify examining stored non-alert data that had been scanned and collected days or even weeks or months before the criminal event, and that may have been scanned at a substantial distance from the site of the crime or intended crime (*e.g.*, at any point along a highway leading to the intended crime site). A spontaneous crime, in contrast, might reasonably justify examination of stored non-alert data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

d. The law enforcement agency shall document the specific crime or related crimes constituting the criminal event and the date(s) and location(s) of the specific crime(s).

### 10.2.3 Crime Trend Analysis

a. A law enforcement agency may access and use stored non-alert data for purposes of conducting crime trend analysis, as that term is defined in these Guidelines, when such access and analysis is approved by a designated supervisor and where such analysis is undertaken to produce analytical products that are intended to assist the agency in the performance of its duties. A designated supervisor may authorize one or more authorized users to conduct a method or methods of crime trend analysis on a repeated or continuous basis, in which event such authorization shall remain in force and effect unless and until modified or rescinded by the supervisor. A designated supervisor may also approve the use of an automated software program to analyze stored data to look for potentially suspicious activity or other anomalies that might be consistent with criminal or terrorist activity.

b. Crime trend analysis of stored non-alert data, whether automated or done manually, shall not result in the disclosure of personal identifying information to an authorized user or any other person unless:

- 1) the agency can point to specific and articulable facts that warrant further investigation of possible criminal or terrorist activity by the driver or occupants of a specific vehicle (*i.e.*, unusual behavior consistent with the *modus operandi* of terrorists or other criminals), and access to the personal identifying information based on those specific and articulable facts has been approved by a designated supervisor. Such approval may be given by a designated supervisor in advance when the crime trend analysis reveals the existence of specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to the authorized user conducting the analysis under the "specific and articulable facts that warrant further investigation" standard of proof established in this Section. The supervisor shall document any and all specified suspicious circumstances for which disclosure of personal identifying information is pre-approved if those suspicious circumstances are revealed by authorized crime trend analysis. When an automated crime trend analysis computer program is used, specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to an authorized user under this Section may also be pre-approved by a designated supervisor and built into the computer program so that if the program identifies the existence of the pre-determined suspicious circumstances, it will automatically alert the authorized user of the suspicious activity and provide to him or her the relevant personal identifying information in accordance with the "specific and articulable facts that warrant further investigation" standard of proof established in this Section; or
- 2) Disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.

c. Nothing in this Section shall be construed to prohibit a computer program from accessing and comparing personal identifying information of one or more individuals who are associated with a scanned vehicle as part of the process of analyzing stored non-alert data, provided that such personal identifying information is not disclosed to a person unless the "specific and articulable facts that warrant further investigation" standard is satisfied. The "specific and articulable facts that warrant further investigation" standard set forth in this Section applies only to the crime trend analysis of non-alert data, and nothing in this Section shall be construed to limit disclosure of personal identifying information of a person who is the registered owner of a vehicle that is on an initial or post-scan BOLO list (*i.e.*, alert data).

d. For the purposes of this Section, the "specific and articulable facts that warrant further investigation" standard required for the disclosure of personal identifying based upon crime trend

analysis of stored non-alert data is intended to be comparable to the “specific and articulable facts that warrant heightened caution” standard developed by the New Jersey Supreme Court in State v. Smith, 134 N.J. 599, 616-19 (1994) (establishing the level of individualized suspicion required before an officer may order a passenger to exit a motor vehicle stopped for a traffic violation).

e. The law enforcement agency accessing stored non-alert ALPR data for purposes of conducting crime trend analysis shall document: the nature and purpose of the crime trend analysis; the persons who accessed stored non-alert ALPR data for use in conducting that analysis; and the designated supervisor who approved access to ALPR non-alert data. In any instance where personal identifying information is disclosed based upon crime trend analysis of stored non-alert data, the agency shall document the specific and articulable facts that warrant further investigation and the designated supervisor who reviewed those facts and approved the disclosure of personal identifying information, or who pre-approved disclosure of personal identifying information based upon specified circumstances identified by an automated crime trend analysis computer program, or, where applicable, the fact that access to personal identifying information was authorized by a grand jury subpoena.

## **11. SHARED LAW ENFORCEMENT ACCESS TO STORED ALPR DATA**

### **11.1 Authorization to Share and Aggregate Data**

Any ALPR data that may in conformance with these Guidelines be accessed and used by the law enforcement agency that collected the data may be shared with and provided to any other law enforcement agency. Stored ALPR data may be combined with ALPR data collected by two or more law enforcement agencies (*e.g.*, collection of stored data by the State Police Regional Operations Intelligence Center), provided that such aggregated data shall only be retained, accessed, and used in accordance with the provisions of these Guidelines.

### **11.2 Record of Shared Access and Responsibilities of the Receiving Agency**

When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the agency that collected the ALPR data shall document the identity of the other agency and the specific officer(s) or civilian employee(s) of that agency who were provided the information. When the transfer of stored ALPR data is done periodically as part of a system for aggregating data collected by two or more law enforcement agencies (*e.g.*, the scheduled and routine transmittal of data to the State Police Regional Operations Intelligence Center), each agency contributing data to the combined database shall maintain a record of the data transfer, which may be an automated record, and shall have and keep on file a memorandum of understanding or agreement or other memorialization of the arrangement for maintaining and populating a database comprised of stored ALPR data collected by multiple law enforcement agencies. Any agency

provided with access to or use of the ALPR data collected by another agency shall comply with all applicable provisions of these Guidelines concerning stored ALPR data and disclosure of personal identifying information.

### **13. RELEASE OF ALPR DATA TO NON-LAW ENFORCEMENT PERSONS OR AGENCIES**

Stored ALPR data shall be treated as "criminal investigatory records" within the meaning of N.J.S.A. 47:1A-1 *et seq.*, and shall not be shared with or provided to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by a subpoena or court order, or unless such disclosure is required by the Rules of Court governing discovery in criminal matters. Any agency receiving a subpoena or court order for the disclosure of ALPR data shall, before complying with the subpoena or court order, provide notice to the County Prosecutor, or to the Division of Criminal Justice in the case of any state-level law enforcement agency.

### **14. PROMULGATION AND ENFORCEMENT OF DEPARTMENTAL POLICIES**

#### **14.1 Required Contents of Departmental Policies**

Pursuant to the requirements of Attorney General Law Enforcement Directive 2010-5, every law enforcement agency that possesses or uses an ALPR must promulgate and enforce a rule, regulation, standing operating procedure, directive, or order that establishes a comprehensive policy governing the operation of ALPRs, and governing access to, use, and retention of all stored ALPR data. The ALPR policy promulgated by the department must be consistent with the standards and procedural safeguards established in these Guidelines, and each ALPR policy must include the following provisions:

a. The ALPR policy shall provide that the chief of the department will designate one or more superior officers to oversee and administer the agency's ALPR program. These designated supervisors will be authorized to: provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data; review and approve requests to access and use stored ALPR data to conduct crime trend analysis and/or to access personal identifying information based upon crime trend analysis; and generally to ensure compliance with the department's ALPR policy and these Guidelines.

b. The ALPR policy shall provide that the chief of the department shall designate all

authorized users, and that no officer or civilian employee will be authorized to operate an ALPR, or to access or use ALPR stored data, unless the officer or civilian employee has received training by the department on the proper operation of these devices, and on the provisions of the department's ALPR policy and these Guidelines.

c. The ALPR policy shall implement and enforce the five-years retention period for ALPR stored data established in Section 9 of these Guidelines, and must provide for the purging of all ALPR stored data at the expiration of the five-year term.

d. The ALPR policy shall provide for the documentation of all ALPR-related activities and decisions that are required to be documented by Section 5 or any other provision of these Guidelines, which may be done by an automated record-keeping system, and shall provide that such records documenting the use of ALPRs and ALPR stored data shall be maintained for 5 years and shall be kept in a place and in a manner as to facilitate a review and audit of the department's ALPR program by the County Prosecutor or by the Attorney General or his or her designee.

e. The ALPR policy shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's policy, or these Guidelines, shall be subject to discipline.

f. The ALPR policy shall provide that all significant violations of the agency's policy, or of these Guidelines, including but not limited to all instances involving the unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor, or to the Director of the Division of Criminal Justice in cases involving a state-level agency, upon discovery of the violation. Unless the County Prosecutor or Director elects to conduct or oversee the investigation of the violation, such notification of the violation shall be followed up with a report, approved by the chief of the department, explaining to the County Prosecutor, or to the Director, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.

#### 14.2 Notice of ALPR Policies and Revisions Provided to County Prosecutors or the Division of Criminal Justice

The chief of the department shall provide a copy of the agency's written ALPR policy to the County Prosecutor, or to the Division of Criminal Justice in the case of a state-level agency, at or before the time of promulgation, and shall provide to the County Prosecutor, or to the Division, copies of any amendments or revisions to the agency's ALPR policy at or before the time that such amendments take effect.

## 15. ALPR PROGRAM ACCOUNTABILITY

### 15.1 ALPR Program Audits

All ALPR records documenting the use of an ALPR, or access to or use of ALPR stored data, whether kept manually or by means of an automated record-keeping system, shall be subject to review and audit by the County Prosecutor, or by the Attorney General or his or her designee.

### 15.2 Handling of Complaints

Any complaints about a department's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor, or to the Director of the Division of Criminal Justice in the case of a State-level agency, for appropriate review and handling. The County Prosecutor, or Director, may conduct an investigation, or may direct the agency that is the subject of the complaint to conduct an investigation and to report back to the County Prosecutor or Director.

## 16. SANCTIONS FOR NON-COMPLIANCE

If the Attorney General or his or her designee has reason to believe that a law enforcement agency or officer or civilian employee is not complying with or adequately enforcing the provisions of these Guidelines, the Attorney General may temporarily or permanently suspend or revoke the authority of the department, or any officer or civilian employee, to operate an ALPR, or to gain access to or use ALPR stored data. The Attorney General or her designee may initiate disciplinary proceedings, and may take such other actions as the Attorney General in his or her sole discretion deems appropriate to ensure compliance with these Guidelines.

## 17. AUTHORITY OF ATTORNEY GENERAL TO GRANT EXEMPTIONS OR SPECIAL USE AUTHORIZATIONS

ALPRs, and all ALPR stored data, shall only be used and accessed for the purposes and in the manner authorized by these Guidelines. In recognition of the need to be able to address issues or circumstances that are not contemplated by these Guidelines, the Attorney General or his or her designee may grant an exemption from any provision of these Guidelines, and may authorize the specific use of an ALPR, or the data collected by or derived from an ALPR, that is not expressly authorized by these Guidelines. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by these Guidelines shall be made to the Attorney



General or his or her designee through the Director of the Division of Criminal Justice or his or her designee, who shall make recommendations on whether to grant the agency's specific request for an exemption or special authorization. Such requests shall be made in writing unless the circumstances are exigent, in which event the request by the agency and approval or denial by the Attorney General or his or her designee may be given orally, in which event the circumstances of the request and the approval or denial shall be memorialized in writing as soon thereafter as is practicable.