NEW BRUNSWICK POLICE DEPARTMENT POLICY & PROCEDURES

VOLUME: 5	CHAPTER: 12	# OF PAGES: 14

SUBJECT: AUTOMATED LICENSE PLATE READERS

BY THE ORDER OF: Anthony A. Caputo Police Director	ACCREDITATION STANDARDS: N/A
Effective Date: **April 10, 2012**	**Date of Last Revision:**

PURPOSE The purpose of this policy is to establish uniform procedures for the use of automated license plate readers (ALPR).

POLICY It is the policy of the New Brunswick Police Department to utilize ALPR technology to the extent possible in accordance with **New Jersey Attorney General's Directive 2010-5**.

PROCEDURES

I. Definitions

A. **Automated License Plate Reader (ALPR)** - means a system consisting of a camera(s) and related equipment that:

1. Automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device;

2. Automatically converts digital photographic images of scanned license plates into electronic text documents;

3. Is capable of comparing scanned license plate text data with data files for vehicles on a BOLO list programmed into the device's electronic memory; and

4. Notifies officers, whether by an audible alert or by other means, when a scanned license plate matches the license plate on the programmed BOLO list.

B. **Authorized user** - means a sworn or civilian employee of a law enforcement agency who has been authorized by the chief law enforcement official of the agency, or by the Attorney General or a county prosecutor or designee, to operate an ALPR or to access and use ALPR stored data, and who has successfully completed training on this policy and on AG Directive 2010-5.

C. **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.

D. **BOLO list** - (also known 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.

1. **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.

2. **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.

E. **Chief** - shall mean the Chief of Police or the highest-ranking sworn officer of a law enforcement agency.

F. **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.

G. **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.

H. **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 subsection IX.F of this policy.

I. **Designated supervisor(s)** - means one or more superior officers assigned by the Director of Police to oversee and administer or to assist in overseeing and administering the agency's use of ALPRs and stored ALPR data.

1. The TSEU Supervisor shall oversee and administer the ALPR Units.

2. The Major Crimes Unit Executive Officer shall oversee and administer queries of stored data.

J. **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.

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

L. **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.

M. **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 (e.g. 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.

1. **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.

2. **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.

3. **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).

II. General

A. ALPR and the data that are collected by these devices stored for future use shall only be used in accordance with Attorney General Directive 2010-5, the manufacturer's use manual, and this policy. ALPRs and ALPR-generated data shall only be used for bona fide public safety purposes.

B. These procedures apply to any ALPR data that is collected by another law enforcement agency and provided to this agency or collected by this agency and provided to another law enforcement agency.

C. An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business and should be interpreted and applied to achieve the following objectives:

1. To ensure that BOLO lists 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;

2. To ensure that data that is 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;

3. 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

4. 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.

D. ALPR shall be used in a consistent manner to assist department personnel in accomplishing its mission in homeland security, suspect interdiction, stolen property recovery, detection of crime, enforcement of State law and local ordinances, identification of stolen vehicles, stolen license plates, wanted and missing persons, AMBER & SILVER Alert assistance, crime prevention and other traffic related matters.

E. Information obtained through ALPR use shall only be released or disseminated in accordance with NJCJIS User Agreement protocols, applicable State Statutes, and applicable Court Rules. Unauthorized release of any information obtained through an ALPR is subject to criminal, civil, and administrative sanctions.

F. ALPR is more than an enforcement tool. ALPR should be deployed to capture the license plates of vehicles in the area of a major crime or an area of repeated minor offenses. Captured data can be analyzed and utilized in criminal investigations or in the assignment of staffing based on empirical data.

G. Designated supervisors shall:

1. 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;

2. Review and approve requests to access and use stored ALPR data to conduct crime trend analyses and/or to access personal identifying information based upon crime trend analyses; and

3. Ensure compliance with this policy and AG Directive 2010-5.

H. The Director of Police shall designate all authorized users. No officer or civilian employee will be authorized to operate an ALPR, or access or use ALPR stored data, unless the officer or civilian employee has received training by the agency on the proper operation of these devices, and on the provisions of this policy and AG Directive 2010-5.

I. Any sworn officer or civilian employee of the agency who knowingly violates this policy or AG Directive 2010-5 shall be subject to discipline.

J. All significant violations of this policy or AG Directive 2010-5, including but not limited to all instances involving the unauthorized access or use of ALPR stored data, must be reported to the Middlesex County Prosecutor's Office upon discovery of the violation. Unless the MCPO 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 Director of Police, explaining to the County Prosecutor the

circumstances of the violation, and the steps that are being taken to prevent future similar violations.

1. Investigations into violations of this policy shall be conducted in accordance with the internal affairs process.

K. The Director of Police shall provide a copy of this policy to the County Prosecutor, at or before the time of promulgation and shall provide to the County Prosecutor copies of any amendments or revisions to this policy at or before the time that such amendments take effect.

III. Deployment of ALPR

A. 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 which 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).

B. Personnel must ensure that the lenses are free from obstructions before operations. If safe to do so, personnel may remove obstructions such as snow, mud, paper, etc. Under no circumstances are the camera lenses to be wiped with anything other than a clean, soft cloth.

C. Any damage to the ALPR systems or any problems with the operation of an ALPR system should be immediately reported to a supervisor verbally and then documented on a Vehicle Inspection Sheet and Interoffice Memorandum and forwarded to the TSEU Supervisor.

D. Personnel authorized to use ALPR shall ensure that the system is operating properly every time the vehicle is used for patrol.

IV. Maintenance of Records

A. The TSEU Supervisor shall maintain a written or electronic record that documents the following information:

1. The vehicles in which the vehicles are mounted and operational;

2. The date and time when the ALPR units were made operational;

3. A list of trained ALPR operators;

B. The MCU Executive Officer shall maintain a record of all access to stored ALPR data. The record shall document the following information:

1. The date and time of access, and in the case of access to stored non-alert data, the type of access authorized (e.g., post-scan BOLO query, crime scene query, or crime trend analysis);

2. The authorized user who accessed the stored data;

3. Whether an automated software program was used to analyze stored data;

4. The supervisor who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required;

5. The supervisor who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying information;

6. Any other information required to be documented.

V. Content and Approval of BOLO Lists

A. 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.

B. 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.

C. Examples of legitimate and specific reasons include, but are not limited to:

1. Persons who are subject to an outstanding arrest warrant;

2. Missing persons;

3. Amber or Silver Alerts;

4. Stolen vehicles;

5. Vehicles that are reasonably believed to be involved in the commission of a crime or disorderly persons offense;

6. 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;

7. Vehicles with expired registrations or other Title 39 violations;

8. 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;

9. 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

10. Persons who are on any watch list issued by a State or federal agency responsible for homeland security.

D. 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.

E. 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 or Silver 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 or Silver Alert expires or is withdrawn.

F. 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.

VI. Actions in Response to an Immediate Alert

A. When officers operating a vehicle equipped with ALPR receive an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. Officer(s) 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. (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).

B. 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.

VII. Security of Stored ALPR Data

A. All ALPR stored data shall be maintained by the Middlesex County Sheriff's Office IT Department. Access to this stored data shall be limited to the MCU Executive Officer or designee and the purposes described in Section IX.

B. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file and if appropriate be placed into evidence in accordance with this department's evidence or records management procedures.

VIII. Retention Period and Purging of Stored Data

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

B. After the retention period has been passed, the data shall be purged from the agency's data storage device or system.

C. ALPR data may be purged 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 AG Directive 2010-5 § 11 and this policy.

D. 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 § 9 of AG Directive 2010-5.

IX. Limitations on Access to and Use of Stored ALPR Data

A. The MCU Executive Officer or designees 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.

1. A record shall be made of all access to ALPR data, which may be an automated record that documents the date of access and the identity of the authorized user.

2. An authorized user does not need to obtain approval from the chief or designated supervisor 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 this policy.

B. Access to and use of stored Non-Alert ALPR Data is limited to the following three purposes:

1. A post-scan BOLO query;

2. A crime-scene query; and

3. Crime trend analysis.

C. An authorized user does not need to obtain approval from the chief or a designated supervisor for each occasion on which he or she accesses and uses stored non-alert data pursuant to this policy.

D. Post-Scan BOLO Query

1. Authorized users are 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.

2. Example: an authorized user 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. Authorized users 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.

E. Crime Scene Query

1. Authorized users are permitted 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.

   a. If an investigator 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 as part of post-scan BOLO query.

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

3. 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. Examples:

   a. 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).

   b. 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.

4. The authorized user shall document the specific crime or related crimes constituting the criminal event and the date(s) and location(s) of the specific crime(s).

F. Crime Trend Analysis

1. An authorized user may access and use stored non-alert data for purposes of conducting crime trend analyses when such access and analyses are approved by the MCU Executive Officer and where such analyses are undertaken to produce analytical products that are intended to assist the agency in the performance of its duties.

   a. The MCU Executive Officer 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.

   b. The MCU Executive Officer 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.

2. Crime trend analyses 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:

   a. 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 *(e.g.* 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. 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 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/her the relevant personal identifying information in accordance with the specific and

articulable facts that warrant further investigation standard of proof; or

b. Disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.

3. 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 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.

4. 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).

5. The authorized user accessing stored non-alert ALPR data for purposes of conducting crime trend analysis shall document:

a. The nature and purpose of the crime trend analysis;

b. The persons who accessed stored non-alert ALPR data for use in conducting that analysis; and

c. The designated supervisor who approved access to ALPR non-alert data.

6. In any instance where personal identifying information is disclosed based upon crime trend analysis of stored non-alert data, the authorized user 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.

X. Shared Law Enforcement Access to Stored ALPR Data

A. ALPR data obtained in conformance with this policy can be accessed and used by this agency and may be shared with and provided to any other law enforcement agencies.

B. 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 AG Directive 2010-5 and this policy.

C. When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the Designated Supervisor 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.

D. When the transfer of stored ALPR data is performed 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 this agency shall comply with all applicable provisions of AG Directive 2010-5 concerning stored ALPR data and disclosure of personal identifying information.

XI. Release of ALPR Data to Non-Law Enforcement Persons or Agencies

A. Stored ALPR data shall be considered criminal investigatory records as defined in NJSA 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.

XII. Program Accountability

A. 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 designee.

B. Any complaints about a department's ALPR program made by any citizen or entity shall be forwarded to the County Prosecutor for appropriate review and handling. The County Prosecutor 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. Investigations into violations of this policy shall be conducted in accordance with the internal affairs process.

XIII. Sanctions for Non-Compliance

A. If the Attorney General or 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 AG Directive 2010-5, 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 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.

XIV. Authority of Attorney General to Grant Exemptions or Special Use Authorizations

A. ALPRs and all ALPR stored data shall only be used and accessed for the purposes and in the manner authorized by AG Directive 2010-5. In recognition of the need to be able to address issues or circumstances that are not contemplated by AG Directive 2010-5, the Attorney General or designee may grant an exemption from any provision of AG Directive 2010-5 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 AG Directive 2010-5. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by AG Directive 2010-5 shall be made to the Attorney General or designee through the Director of the Division of Criminal Justice or 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 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.