State of New Jersey
OFFICE OF THE ATTORNEY GENERAL
DEPARTMENT OF LAW AND PUBLIC SAFETY
DIVISION OF CRIMINAL JUSTICE
PO BOX 085
TRENTON, NJ 08625-0085
TELEPHONE: (609) 984-6500

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

MATTHEW J. PLATKIN
Attorney General

PEARL MINATO
Director

ATTORNEY GENERAL LAW ENFORCEMENT DIRECTIVE NO. 2022-12

TO: All Law Enforcement Chief Executives and County Prosecutors

FROM: Matthew J. Platkin, Attorney General

DATE: October 21, 2022

SUBJECT: Updated Directive Regulating Use of Automated License Plate Recognition (ALPR) Technology

In 2010, Attorney General Law Enforcement Directive 2010-5 established statewide guidelines governing the use of automated license plate recognition (ALPR) technology and the data it generates.[1] After more than a decade of experience with what was then an emerging technology, an updated policy on ALPRs is necessary.

This update has two major goals. First, it maintains—and builds upon—the significant safeguards from abuse and privacy protections that have served the State well under the 2010 policy, including continuing to apply the New Jersey Supreme Court's framework in State v. Donis, 157 N.J. 44 (1998), limiting law enforcement access to personal identifying information associated with a vehicle's license plate unless there is a particularized basis. Second, the revised policy facilitates the sharing and standardization of ALPR data statewide in order to maximize our ability to use this tool to solve and prevent crimes.

The major revisions are as follows. Additionally, other portions of the 2010 policy have been reorganized or condensed.

- ***Oversight***. Establishes ALPR coordinators at the agency, county, and state level to improve oversight and information sharing.

- ***Sharing and standardization of data***. Requires use of the statewide application program

[1] "Automated license plate recognition" or ALPR is technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. ALPR devices may be placed at a stationary location (permanent or portable) or be mobile and affixed to a police vehicle. The vehicle location data captured by an ALPR device is (1) used to alert law enforcement to vehicles they have a legitimate and specific reason to locate, and (2) stored so that law enforcement may perform searches to further subsequent investigations. Both situations are described in more detail in this Directive.

interface ("Statewide API")—software that will make ALPR data accessible statewide—and mandates standard data formats to make ALPR information consistent across agencies, without requiring additional agreements between agencies.

- ***Retention period***. Decreases retention period for both ALPR data and records from five years to three years.

- ***Release of ALPR data***. Lays out release process for ALPR data in criminal prosecutions.

- ***Audits***. Mandates annual audits of each agency's ALPR program.

- ***Training***. Establishes specific training requirements for all agency users authorized by their law enforcement executive to use ALPRs and access ALPR data.

Therefore, pursuant to the authority granted to me under the New Jersey Constitution and the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 to -117, which provides for the general supervision of criminal justice by the Attorney General as chief law enforcement officer of the State in order to secure the benefits of a uniform and efficient enforcement of the criminal law and the administration of criminal justice throughout the State, I hereby direct all law enforcement and prosecuting agencies operating under the authority of the laws of the State of New Jersey to implement and comply with the directives outlined below.

1. **Oversight**

1.1 ***Agency***. The law enforcement executive of each agency using an ALPR or its data shall designate an Agency ALPR Coordinator who will:

- Be the external point of contact for agency ALPR-related items such as information sharing and audits;

- Internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors);

- Designate authorized users within the agency who can use ALPRs and access stored data (such users must complete the trainings mandated by this Directive).

1.2 ***County***. Each County Prosecutor will designate a County ALPR Coordinator who will maintain contact information for Agency ALPR Coordinators in the county and provide it to the State ALPR Coordinator. Where county ALPR data is maintained by a sheriff's department or public safety agency, a representative from that agency may be designated as a County ALPR Co-Coordinator. State agencies should report their Agency ALPR Coordinators directly to the State ALPR Coordinator.

1.3 ***State***. The Attorney General, in consultation with the New Jersey State Police ROIC Commander, will designate a State ALPR Coordinator to oversee the "Statewide API" that connects stored ALPR data (discussed below) and the state's ALPR program generally.

2. Deployment

2.1 ***Official use only***. An ALPR and the data it generates shall only be used for official and legitimate law enforcement purposes. The agency's law enforcement executive or designee must authorize deployment of each ALPR.

2.2 ***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, 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).

2.3 ***Sharing deployment information***. The following data must be shared with the State ALPR Coordinator prior to installing or relocating a permanent fixed ALPR unit:

- Camera name (pursuant to convention specified by State ALPR Coordinator)
- Location (latitude and longitude)
- Survey provided by ALPR vendor, including projected size of ALPR data

When deploying or relocating a portable fixed ALPR unit, agencies must provide updated latitude and longitude data to the State ALPR Coordinator.

2.4 ***Deconfliction***. Agency ALPR Coordinators shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.

3. BOLO lists

3.1 ***Standard for including license plate in BOLO list***. A license plate number may be included in a "be on the lookout" or BOLO list (a compilation of license plates or partial plates for which a BOLO situation exists) for input into an ALPR system only if there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person(s) 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/SILVER alerts
- Vehicles and/or persons involved in prior suspicious activity, such as groups of vehicles travelling together suspected of criminal activity, or subjects trying to open doors to random cars
- Stolen vehicles
- Vehicles reasonably believed to be involved in the commission of a crime or disorderly persons offense
- Vehicles registered to or 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
- Persons who are on any watch list issued by a state or federal agency responsible for homeland security

3.2 ***Batch downloading***. 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, US Department of Homeland Security, and Motor Vehicle Commission database.

3.3 ***Updating BOLO lists***. A BOLO list may be revised at any time. Updates to a BOLO list shall be done at the start of each shift for mobile ALPRs attached to police vehicles, and as frequently as possible, but at least daily, for ALPRs at stationary locations.

3.3.1 All ALPR systems must provide an Application Program Interface (API) or web service to update in real-time a BOLO list(s) through methods approved by the State ALPR Coordinator, including AMBER/SILVER alerts that remain on the list until expired or withdrawn.

3.4 ***Immediate alert response***. A BOLO match with an ALPR scan may be programmed to trigger an immediate alert. The reason for including the vehicle on the BOLO list shall be disclosed to the officer who will react to an immediate alert. The officer should determine whether the alert has been designated as a non-encounter alert (meaning officer should not encounter the vehicle) and, if so, follow any instructions included in the alert for notifying the originating agency.

3.4.1 When an officer receives an immediate alert without a non-encounter restriction, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted 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 NJ. Super. 407 (App. Div. 1996) (no reasonable suspicion to justify a stop because registered car owner's license suspended unless driver generally matches the owner's physical description (e.g., age and gender)).

4. Accessing stored data

4.1 ***Alert data***. An authorized user may access and use stored ALPR alert data (i.e., ALPR license plate data matching an entry on a BOLO list) as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a BOLO query, a crime scene query, or crime trend analysis (as defined below).

4.2 ***Non-alert data***. Access to and use of stored non-alert ALPR data (i.e., ALPR data gathered not matching a BOLO list entry) is limited to the following three purposes explained below: a BOLO query, a crime-scene query, and crime trend analysis (system tests and troubleshooting are also acceptable purposes).

4.2.1 BOLO query. Agencies may compare a BOLO list against stored non-alert 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 subsequently be placed on an active BOLO list (for example, may review data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned to check an alibi defense or to develop lead information for the purpose of locating a specified vehicle or person; or to determine whether a vehicle that was only recently added to a BOLO list had been previously observed in the jurisdiction before being placed on the list).

4.2.2 Crime scene query. Agencies may 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 (i.e., incident that would constitute an indictable crime under New Jersey law). Such queries may not be conducted to review data based on general crime patterns (e.g., to identify persons traveling in or around a "high crime area"). A record shall be kept of the specific crime(s) justifying the query, including the crime date and location.[2]

4.2.3 Crime trend analysis. Agencies may access and use stored non-alert data where such access, which may be automated, might reasonably lead to the discovery of evidence or information relevant to an investigation that is not related to a specific criminal event. Such access must be approved by the Agency ALPR Coordinator or their designee.

Crime trend analysis shall not result in the disclosure of personal identifying information (such as name, address, SSN, vehicle operator's license number) to an authorized user or any other person unless (a) there exist "specific and articulable facts that warrant further investigation" of possible criminal or terrorist activity by the driver or occupants of a specific vehicle and access has been approved by a designated supervisor; or (b) disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.[3]

---

[2] A crime scene query shall be limited in scope to 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 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). In contrast, a spontaneous crime might reasonably justify examining data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

[3] 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

Any crime trend analysis shall document:

- The nature and purpose of the crime trend analysis
- The authorized users who accessed stored non-alert data
- The designated supervisor who approved access
- Where personal identifying information was disclosed, (a) the specific and articulable facts that warrant further investigation and (b) the designated supervisor who approved the disclosure of personal identifying information; or, where applicable, the fact that a grand jury subpoena authorized access to personal identifying information.

4.3 ***Documenting access for any stored data search***. A record shall be made of the authorized user accessing stored ALPR data and the date, and for non-alert data the record should include the justification for access. Once stored data has been accessed and transferred to an investigation file by an authorized user, it shall not be necessary after that to document further access or use of that data pursuant to this Directive.

5. Sharing data

5.1 ***Statewide API***. The State ALPR Coordinator shall implement a "Statewide API" (application program interface) that allows access to stored ALPR data across agencies, and specify the method by which all ALPRs used by New Jersey agencies must provide real-time access to ALPR data through the API. Agencies may also share data regionally with other New Jersey agencies pursuant to the mandates of this Directive, and ALPR data collected by a private entity that has entered into an agreement with New Jersey law enforcement can be shared with New Jersey agencies. All ALPRs must make data available to the Statewide API by the effective date of this Directive, and subsequent ALPRs must do so within 45 days of deployment. ALPR systems must be programmed to capture data parameters and meet minimum requirements for accuracy and performance as specified by the State ALPR Coordinator.

5.2 ***Sharing with agencies not covered by this Directive***. An agency may enter into a written agreement to share ALPR data with, or receive data from, a law enforcement agency outside of New Jersey or otherwise not covered by this Directive with the approval of the State ALPR Coordinator. Only federally recognized law enforcement agencies may receive access to a New Jersey agency's ALPR data. The State ALPR Coordinator may agree to share ALPR data with a law enforcement agency outside of New Jersey if the out of state agency agrees in writing to use the data only for documented, legitimate law enforcement purposes and to follow other restrictions required by the State ALPR Coordinator in order to achieve 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).

objectives of this Directive. Private entities may provide ALPR data to New Jersey agencies but cannot receive law enforcement-owned ALPR data.

6. Storage, records, and retention

6.1 ***Storage of ALPR data***. All ALPR data shall be stored securely and maintained electronically with access restricted to authorized users. ALPR data shall be the property of the agency and not any ALPR vendor. Agencies may jointly store their ALPR data. Commercially obtained ALPR data shall not be co-mingled with law enforcement data. Data being used in an investigatory process shall be maintained in accordance with the agency's evidence or records management procedures.

6.2 ***Deployment records***. Agencies shall maintain the following information regarding each ALPR owned or operated:

- Date and time deployed
- Portable or fixed
- Identity of operator
- Vendor name
- Date ALPR data connected to Statewide API (for agencies that house ALPR data)

6.3 ***Stored ALPR data access records***. Agencies that store ALPR data shall maintain an automated record-keeping of all access to stored ALPR data (in the case of county storage, the county may keep access records instead), including the following:

- Date and time of access, and for non-alert data, the justification for access
- Authorized accessor name
- Whether an automated software program was used to analyze the data
- Designated supervisor who approved disclosure of personal identifying information based upon crime trend analysis
- Instances of testing or troubleshooting an ALPR system
- Any other information required to be documented under this Directive

6.4 ***Retention***. Records and ALPR data covered by this Section shall be retained for three years.

6.4.1 ALPR stored data shall be purged after the retention period, unless it is associated with an active investigation or pending judicial process, in which case the data should be exported from the relevant storage system and retained in the case file.

6.4.2 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 required retention and purging period.

6.4.3 Records shall be kept in a manner that makes them readily accessible for audit.

7. Discovery

7.1 ***Criminal investigatory records***. 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 a subpoena or court order authorizes such disclosure or unless such disclosure is required by court rules governing discovery in criminal matters.

7.1.1 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 Director of the Division of Criminal Justice (DCJ)).

7.2 ***Release of ALPR data***. If ALPR data is accessed as part of an investigation—including but not limited to a BOLO query, a crime scene query, or crime trend analysis—a record of the access, which may be automated, and corresponding data shall be included in the agency's investigative file (electronic or physical). If the investigation results in criminal charges, the ALPR records shall be turned over in discovery pursuant to applicable court rules and case law.

8. Compliance

8.1 ***Establishing a policy***. Agencies that possess or use an ALPR or its data shall establish—or conform existing—standing operating procedures, directives, or orders that govern ALPRs and stored ALPR data consistent with this Directive before the Directive takes effect (ninety days after issuance). The law enforcement executive shall provide a copy of the agency's ALPR policy to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator at or before the time of promulgation, including any subsequent policy amendments.

8.2 ***Violations***. Any knowing violation of this Directive or related agency standing operating procedure, directive, or order, or applicable law, shall be subject to discipline.

8.2.1 All significant violations of this Directive or agency policy, including but not limited to unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator upon discovery. 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 law enforcement executive and with notification to the State ALPR Coordinator, 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.

8.2.2 Any complaints about an agency's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor (or DCJ Director), for appropriate review and handling, as well as notification to the County and State ALPR Coordinator. The County Prosecutor or Director may conduct an investigation or direct the agency that is the subject of the complaint to conduct an investigation and

report back to the County Prosecutor or Director, with notification to the State ALPR Coordinator.

8.2.3 If the Attorney General or their designee has reason to believe that a law enforcement agency is not complying with or adequately enforcing the provisions of this Directive, 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 their sole discretion, deems appropriate to ensure compliance with this Directive.

8.3 ***Audits***. By January 31 each year, the Agency ALPR Coordinator shall perform an audit of their agency's ALPR program and provide it to the County and State ALPR Coordinator.[4] That audit shall certify the following:

- Agency has an ALPR policy in place
- Only authorized users have accessed ALPR data
- Date of each authorized user's last ALPR training
- That a random survey of ALPR accesses revealed no misuse
- A description of any known significant violations and citizen complaints and whether they have been forwarded to the County Prosecutor or DCJ Director

The County ALPR Coordinator or State ALPR Coordinator may conduct an audit of an agency's ALPR program at any time.

8.4 ***Public reporting***. By March 31 each year, the State ALPR Coordinator shall publicly report the list of agencies that have completed audits, and the number of significant violations and citizen complaints reported by each agency.

8.5 ***Training***. The State ALPR Coordinator shall design and disseminate training on ALPR technology—including the application of this Directive and privacy and security considerations generally—that shall be a prerequisite for an individual being designated an authorized user under this Directive. Authorized users must complete refresher trainings every two years, as determined by the State ALPR Coordinator.

9. <u>Other provisions</u>

9.1 ***Attorney General exemptions***. ALPRs, and all ALPR stored data, shall only be used and accessed as authorized by this Directive. However, the Attorney General or their designee may authorize the specific use of an ALPR or the data it generates that is not expressly authorized by this Directive. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by this Directive shall be made to the Attorney General or their designee through the DCJ Director. Such requests shall be made

[4] Where appropriate, a County Prosecutor may perform an agency's audit in place of the Agency ALPR Coordinator. The State ALPR Coordinator will audit the New Jersey State Police ALPR program.

in writing unless the circumstances are exigent, in which case approval or denial may be given orally and memorialized in writing as soon thereafter as is practicable.

9.2 ***Non-enforceability by third parties***. This Directive is issued pursuant to the Attorney General's authority to ensure the uniform and efficient enforcement of the laws and administration of criminal justice throughout the State. This Directive imposes limitations on law enforcement agencies and officials that may be more restrictive than the limitations imposed under the United States and New Jersey Constitutions, and federal and state statutes and regulations. Nothing in this Directive shall be construed in any way to create any substantive right that may be enforced by any third party.

9.3 ***Severability***. The provisions of this Directive shall be severable. If any phrase, clause, sentence or provision of this Directive is declared by a court of competent jurisdiction to be invalid, the validity of the remainder of the document shall not be affected.

9.4 ***Questions***. Any questions concerning the interpretation or implementation of this Directive shall be addressed to the DCJ Director or their designee.

9.5 ***Effective date***. This Directive shall take effect on January 23, 2023, which is approximately ninety days after issuance. The provisions of this Directive shall remain in force and effect unless and until it is repealed, amended, or superseded by Order of the Attorney General.

9.6 ***Prior directives***. This Directive supersedes any prior directive on this topic, including Law Enforcement Directive 2010-5 and its November 18, 2015 revision.

Matthew J. Platkin
Attorney General

ATTEST:

Lyndsay V. Ruotolo
First Assistant Attorney General

Dated: October 21, 2022