

ALPR Policy Guidelines

Each law enforcement agency that uses ALPR should implement a policy governing the operation, use, administration, and oversight of ALPR systems (hereinafter, “ALPR Policy”). The ALPR Policy should address, at minimum, the following foundational requirements:

Oversight & Administration

- Designate personnel to be responsible for administering and overseeing the ALPR program and system.
- Require regular (no less than quarterly) reporting to police oversight board on ALPR system use that includes metrics re: use, cost, hit rate, false positive rate, and arrests/incidents related to ALPR use.
- ALPR system access and use should be authorized by chief executive of the agency on a user-by-user basis.
- Develop and implement procedures for granting and managing user accounts.
- Create user IDs that correspond to specific individuals (no generic or “guest” ID creation) and a process for removing inactive users and require strong passwords. Require that usernames and passwords for accessing the ALPR system are not transferrable, must not be shared by personnel, and must be kept confidential.
- Use of the ALPR system should be monitored and audited regularly to ensure security of the information, compliance with applicable laws, and compliance with policy.
- Designate a single location (e.g., a folder on a network drive) that ALPR images can be downloaded and retrieved.
- Establish a maximum data retention period (suggested: ~90 days at the most) for downloaded ALPR images.
- Establish guidelines for sharing ALPR images with other agencies and third parties. At minimum, require that recipients of ALPR images certify that they will delete the data within a given period of time and shall not share or use the data for any purpose without your prior written approval.
- Specifically require consideration of nondiscriminatory intent in the placement of ALPR cameras.

Training & Accountability

- Require users of the system to receive training on permissible use of the system prior to gaining access.
- Training should include permissible uses of the ALPR system, security and privacy protections on the use of the technology, and the impact and sanctions (see below) for non-permitted uses and/or violations of ALPR policy. Training should also include adequate guidance on:
 - ALPR verification process for law enforcement alerts;
 - Responsibilities and obligations under applicable federal, state, or local law and policy when using the ALPR system;
 - Mechanisms for reporting violations of ALPR policy provisions; and
 - Nature and possible penalties for ALPR policy violations, including possible transfer, dismissal, criminal liability, etc.
- Designate an external individual or entity with privacy, civil rights/civil liberties expertise to receive reported errors and violations and help maintain external oversight of implementation of ALPR privacy, civil rights, and civil liberties protections.
- Specify mechanism for users or other personnel to report errors and suspected or confirmed violations of ALPR policy.

Permissible Use

- ALPR system should be accessible only to users who need the data to fulfill a specific criminal justice purpose.
- ALPRs and data generated by ALPRs must be collected, accessed, and/or used only for a specific criminal justice purpose (i.e., a clearly defined objective for using the ALPR system). The policy should expressly prohibit use of ALPR system for any purpose not expressly enumerated.
 - *Note:* Policy should specifically identify the specific criminal justice purposes for using the ALPR system and collecting data. In order to access the system, users must be required to first (1) select from the list of specific criminal justice purposes (e.g., recovery of stolen vehicles, identifying vehicles used in commission of crime, locating vehicle believed to be driven by dangerous criminal, etc.), and (2) enter a case number.
- Agencies should maintain recordkeeping practices (i.e., comprehensive audit logging) that document all deployments and uses of the ALPR system, as well as sharing of ALPR data with other governmental agencies. Good recordkeeping will support efforts to properly manage ALPR system implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help evaluate usefulness of ALPR system.
 - *Note:* When logging uses of the system, the log should capture, at minimum, the user ID, date of access, permissible use, case number, any notes, and any footage downloaded from the system.
- Users must specify a purpose when downloading or saving ALPR footage (e.g., for evidence).

- All purposes other than a specific criminal justice purpose are to be prohibited (in other words, identify the permissible uses for the ALPR system, and prohibit all others).
- Identify what ALPR information may not be sought, retained, shared, or disclosed.

Data Integrity

- Specify security and privacy controls needed to ensure that downloaded ALPR data is not altered, changed, or improperly disclosed before it is purged.
- Identify procedure that must be followed to validate ALPR data prior to law enforcement action.
- Specify procedure for reviewing alleged or suspected errors and deficiencies of ALPR data (or process for requesting that the vendor investigates).
- Include process for notifying other government agencies when it has been confirmed that ALPR data is erroneous or deficient.
- Identify procedure for providing necessary public notification in the event of a security incident.

Transparency & Audit

- Conduct and publish regular (at least monthly) audit reports of ALPR use to ensure compliance with law and policy.
- Disclose location of all ALPR devices, and provide public notice if they are being relocated.
- Disclose metrics and outcomes re: the cost, expense, and use of ALPR systems to the public on a regular basis.
- Perform a public policy evaluation, prior to publishing, to determine whether the policy adequately addresses current standards, privacy protection recommendations, and the law.
- Perform an annual policy review to consider appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable law, technology, and public expectations.
- Ensure that policy cannot be modified or changed without public notice and input.
- Designate point of contact for handling inquiries and complaints relating to the ALPR system and its uses.

#