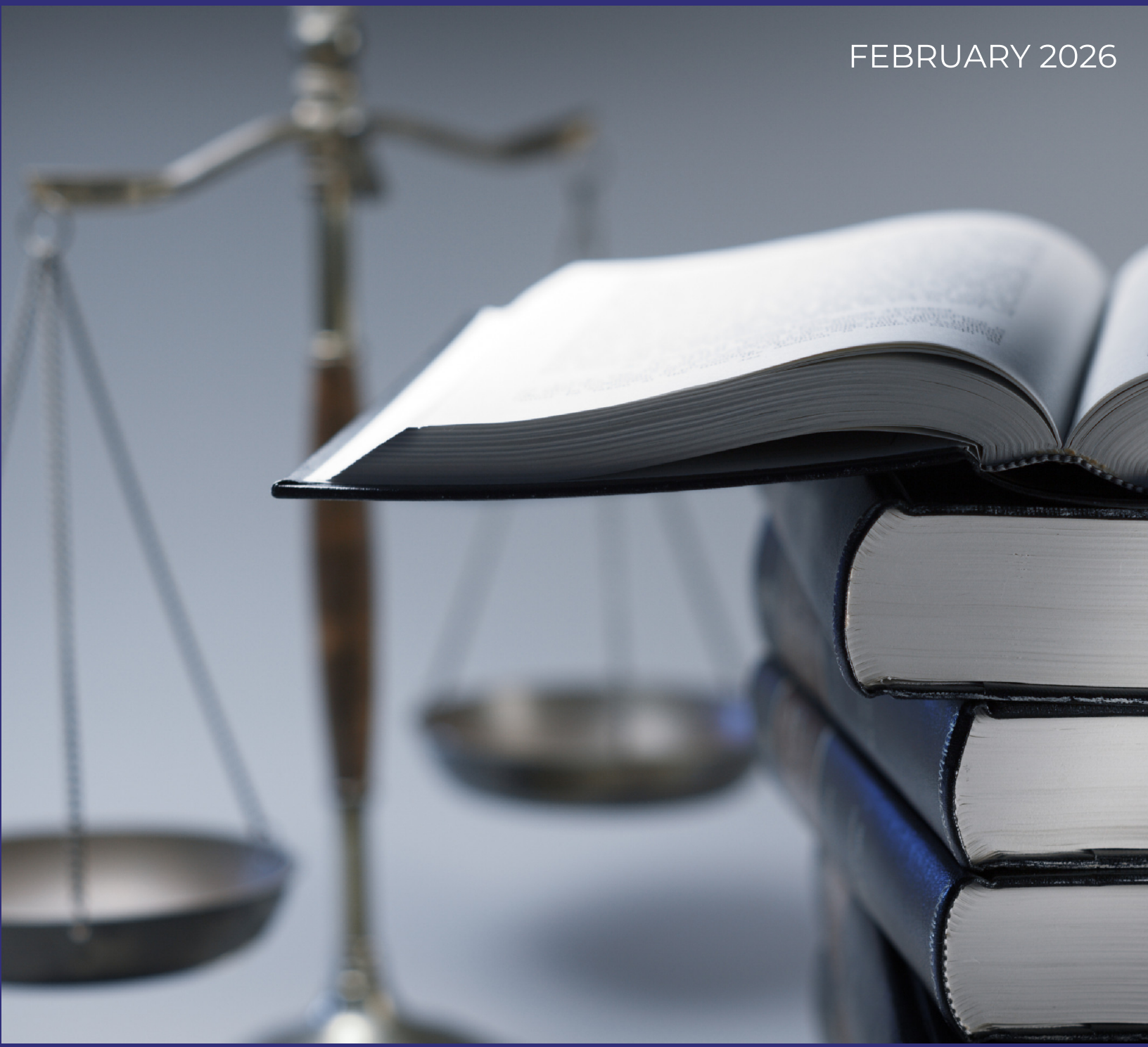
LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION

MODEL AUTOMATIC LICENSE PLATE RECOGNTION SYSTEM ACT

FEBRUARY 2026



LAPPA
LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION

This project was supported by the Model Acts Program, funded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is Current as of February 2026.

MODEL AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM ACT

ACKNOWLEDGMENTS

The Legislative Analysis and Public Policy Association (LAPPA) is grateful to the Office of National Drug Control Policy for its support in funding, enabling, and contributing to this Model Act.

This Model Act could not have been developed without the valuable input of the Model License Plate Recognition System Act working group. LAPPA wishes to thank its distinguished members, four of whom are listed below, for providing the expertise, guidance, and suggestions that contributed to the model's development.

Mike McDaniel
Houston High Intensity Drug Trafficking Area (HIDTA)

Captain Adam Polhemus
New Jersey Statewide Networked ALPR Program (NJ SNAP), New Jersey State Police

Catherine A. Miller
National Capital Region Law Enforcement Information Exchange Program (NCR-LInX)

James Sheehan
Newark/Jersey City Urban Area Security Initiative

MODEL AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM ACT

TABLE OF CONTENTS

Return to Table of Contents

SECTION I. TITLE.

This Act may be cited as the "Model Automatic License Plate Recognition System Act," "Model Act," or "the Act."

SECTION II. LEGISLATIVE FINDINGS AND PURPOSE.

(a) Legislative findings.—The [legislature][1] finds that:

(1) Automatic license plate recognition systems capture photographic images and/or videos of passing vehicles in publicly accessible places and detect information regarding those vehicles including license plate numbers and the vehicle make, model, and color;[2]

(2) Automatic license plate recognition systems also capture the global positioning system location data linked to the automatic license plate recognition system camera that takes the photograph and the date and time the photograph was taken;

(3) Automatic license plate recognition systems are used for a variety of public health and safety purposes including, but not limited to:

(A) Developing leads when attempting to locate missing individuals, including vulnerable children and adults;

(B) Assisting law enforcement with evidence collection and generating investigative leads during efforts to apprehend suspects and locate stolen vehicles;

(C) Assisting law enforcement in drug trafficking and human trafficking investigations; and

(D) Developing leads when attempting to locate individuals who are the subject of an arrest warrant;[3]

(4) According to a 2020 survey from the Bureau of Justice Statistics, 90 percent of sheriffs' offices with 500 or more sworn officers and 100 percent of police departments serving more than one million residents reported using automatic

[1] This Act contains certain bracketed words and phrases (*e.g.*, "[legislature]"). Brackets indicate instances where state lawmakers may need to insert state-specific terminology or facts.
[2] Kristin Finklea, *Law Enforcement and Technology: Use of Automated License Plate Readers*, CONG. RSCH. SERV. 1-2 (Aug. 19, 2024), https://www.congress.gov/crs-product/R48160.
[3] *Id*. at 2-3.

Return to Table of Contents

license plate recognition systems;[4]

(5) Public and private schools, as well as private sector entities like homeowners' associations, banks, parking garages, and retail businesses, also use automatic license plate recognition systems for many purposes, including security, crime deterrence, consumer marketing, parking management, recovering stolen vehicles, vehicle repossession, and investigating insurance fraud;[5]

(6) Automatic license plate recognition systems implicate privacy, data collection, and data security concerns that statewide legislation can address; and

(7) The use of automatic license plate recognition systems is a common sense approach to efficiently assist law enforcement in maintaining community safety.

(b) Purpose.—The purpose of this Act is to:

(1) Establish the governmental entities authorized to use automatic license plate recognition systems;

(2) Establish how data captured by or derived from automatic license plate recognition systems can be used by governmental entities;

(3) Require governmental entities to establish policies for access to and use of automatic license plate recognition systems and data captured by or derived from such systems;

(4) Establish data retention, data collection, and data reporting requirements for governmental entities that use automatic license plate recognition systems;

(5) Require governmental entities that use automatic license plate recognition system data to establish policies setting forth, among other things, how such data can be used; and

(6) Establish penalties for governmental entities who violate this Act or any rules or regulations adopted pursuant to this Act.

[4] *Id*. at 1.

[5] *See* Noah Stein, *Automated License Plate Readers: Legal and Policy Evaluation*, UNIV. OF MICH. GERALD R. FORD SCH. OF PUB. POL'Y (Jan. 2023), https://stpp.fordschool.umich.edu/research/policy-brief/automated-license-plate-readers-legal-and-policy-evaluation; *Guide to License Plate Reader Cameras*, DRN (accessed Feb. 20, 2026), https://drndata.com/blog/guide-to-license-plate-reader-cameras/.

Return to Table of Contents

Commentary

Automatic license plate recognition systems (ALPRs)[6] "are camera systems that capture license plate data of vehicles, along with related information."[7] ALPR cameras are available in fixed, mobile, and portable applications.[8] Fixed cameras are those cameras that are mounted to a fixed location, typically using existing infrastructure (*e.g.*, light poles, traffic lights, and public or private buildings).[9] Mobile systems are typically mounted on police or private contracted vehicles, while portable systems are those cameras that are not mounted to a vehicle but can be moved from location to location, such as a "quick-deploy" camera or an ALPR "trailer" that may also capture a vehicle's speed.[10]

ALPR systems automatically capture images or videos of all vehicles that pass the camera if the system algorithm detects what it determines to be a license plate.[11] A computer algorithm then converts the image or video into computer-readable data, or ALPR readable-data, that includes the license plate number and any additional information the system is set up to detect including, but not limited to, global positioning system (GPS) location data for the camera that took the photograph or video; vehicle make, model, and color; date and time; and other information such as the agency name and site identification.[12] Once the information has been captured and cataloged by the ALPR system, the system can then compare those "data points against various databases, including 'hot lists,' which contain a list of license plate characters linked to vehicles of interest. If there is a match to a 'hot list' license plate, the ALPR system can alert a law enforcement officer in real time."[13] A "hot list" is a list of license plate characters associated with vehicles of interest and includes information on vehicles that originally appear on a "be on the lookout" (BOLO) list[14] and can also include information on vehicles related to kidnappings, AMBER alerts, stolen vehicles, and other criminal activities including potential terrorist activity.[15] In addition to unsolicited notifications from an ALPR system, law enforcement users can manually query the system for investigative purposes, such as to find past

---

[6] Automatic license plate recognition systems are known by a variety of other names including license plate readers, automatic or automated number plate recognition systems, automatic license plate recognition technology, automatic vehicle identification, car plate recognition, and vehicle license plate recognition or identification systems.
[7] Peter G. Berris, Kristin Finklea, and Dave S. Sidhu, *Automated License Plate Readers: Background and Legal Issues*, CONG. RSCH. SERV. 1 (July 21, 2025), https://www.congress.gov/crs-product/IF13068.
[8] *Id*. *See also* Colin L. Drabert, "Law Enforcement Use of Technology: Automatic License Plate Recognition (ALPR)," presented at the Virginia State Crime Commission, Nov. 14, 2024, https://studiesvirginiageneralassembly.s3.amazonaws.com/meeting_docs/documents/000/002/458/original/VSCC_ALPR_Dec_3_JCOTS.pdf?1733235622.
[9] Berris et al., *supra* note 7.
[10] *Id*. *See also* Drabert, *supra* note 8 and *Northern California Fusion Center has 3 Covert ALPR Trailers to Loan Out*, THE CTR. FOR HUM. RTS. AND PRIV., https://www.cehrp.org/tags/lpr-speed-trailer/.
[11] Berris, et al., *supra* note 7.
[12] *Id*. Note that most ALPR systems are predominantly installed to capture rear license plate data and, although it may occur in practice, capturing images of drivers and/or passengers is accidental and not the intended purpose of the system, and such images cannot be used to identify specific individuals.
[13] *Id*.
[14] "'BOLO' or 'Be on the Lookout' 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." *Automatic License Plate Reader (ALPR)*, GRANDVIEW HEIGHTS POLICE GEN. ORDS. (rev. May 9, 2022), https://grandviewheights.gov/DocumentCenter/View/7126/391-Automatic-License-Plate-Reader.
[15] Finklea, *supra* note 2.

Return to Table of Contents

locations where a vehicle of interest has been seen over a period of time.[16] Depending on the system, ALPR data may be queried using a full or partial license plate characters, a description of the vehicle, and by querying the license plate characters or vehicles that appear a similar location at the same time.[17] In either instance, when adding a vehicle to a "hot list" or conducting a manual query of ALPR data, authorized users should provide a legitimate reason (purpose and justification) and law enforcement report number, if applicable.

ALPR data is also used by government entities for enforcement of parking laws, toll collection, and analysis of traffic patterns.[18] Additionally, private individuals and entities use ALPR systems for a range of commercial purposes as well as neighborhood and home security purposes. Non-governmental use of ALPR systems includes parking enforcement in private lots and by homeowners' associations, consumer marketing, enabling repossession of vehicles with past-due car loans where the lender has a contractual right to repossess a vehicle, recovering stolen vehicles, and investigating insurance fraud.[19]

In some states with existing ALPR laws, ALPR data held by law enforcement can be shared with other governmental entities, including other law enforcement agencies; however, some states and entities allow broader sharing (*e.g.*, with federal and/or out-of-state law enforcement agencies) or place limits on data sharing.[20] For example, some federal law enforcement agencies require state and local law enforcement agencies to sign a memorandum of understanding or data sharing agreement in order to access ALPR system data held by that agency.[21] In New Jersey, pursuant to the New Jersey Attorney General Law Enforcement Directive, in-state sharing of ALPR data is mandated for all law enforcement agencies and data sharing agreements must be in place to share ALPR data with out-of-state law enforcement agencies.[22] By contrast, Virginia does not permit law enforcement agencies not located within the commonwealth to access ALPR data while Minnesota requires law enforcement to obtain a warrant to use ALPR data if such data is being used to "monitor or track an individual who is the subject of an active criminal investigation."[23] However, the use of ALPR systems by non-governmental entities is generally unregulated because the nature of ALPR data – a photograph of an object in a publicly accessible place – that is created by a private entity can implicate the freedom of speech protections of the First Amendment. Therefore, access by a governmental

[16] Berris et al., *supra* note 7.
[17] Drabert, *supra* note 8.
[18] *Automatic License Plate Recognition Systems: Summary of State Laws*, LEGIS. ANALYSIS & PUB. POL'Y ASS'N (Sept. 2025), https://legislativeanalysis.org/automatic-license-plate-recognition-systems-summary-of-state-laws/.
[19] *See* Ángel Díaz and Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use,* BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.
[20] LAPPA, *supra* note 18.
[21] *See Privacy Impact Assessment for the National License Plate Reader Program (NLPRP) and DEA Special Intelligence Link (DEASIL)*, DRUG ENF'T ADMIN. 2 (Dec. 20, 2024), https://www.dea.gov/sites/default/files/2025-01/DEA%20NLPRP%20DEASIL%20PIA%20Revision%20-%20Final%2020241220.pdf.
[22] *Attorney General Law Enforcement Directive No. 2022-12*, OFC. OF THE ATT'Y GEN. 6 (Oct. 21, 2022), ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-(ALPR)-Technology.pdf.
[23] VA. CODE ANN. § 2.2-5517(F) (West 2025) and MINN. STAT. ANN. § 13.824 (West 2025). *See also* Drabert, *supra* note 8.

Return to Table of Contents

entity to ALPR data held by a private entity is not typically addressed.[24] Utah law, however, requires law enforcement to obtain a warrant before it can access ALPR data held by a private individual or entity.[25]

As mentioned in the legislative findings, use of ALPR systems is widespread across the country and, as a general rule, individuals have no expectation of privacy in their license plate as it is publicly displayed. However, certain usage of ALPR systems by law enforcement may implicate the Fourth Amendment's prohibition against unreasonable search and seizure.[26] In 2009, the International Chiefs of Police (IACP) released a report that expressed concern that the use of ALPR systems might have "… a chilling effect on social and political activities."[27] Then, in 2013, the American Civil Liberties Union (ACLU) contended that the use of ALPRs infringes on privacy and can be used for mass surveillance and location tracking.[28] In that report, the ACLU observed that its most significant concerns related to the growing use of ALPR systems by law enforcement, a lack of regulation, and the potential for abuse, noting that ALPRs can potentially capture "location data [that] can reveal extremely sensitive information about who we are and what we do."[29] A subsequent report released by the IACP in 2024 pointed out that "technology has made tremendous progress and will continue to evolve in the future," but that "the benefits of any technology and any data collection must be considered against potential risks of harm including potential violations of individual rights and liberties."[30]

State and federal courts analyzing ALPR claims "have almost uniformly concluded that neither taking photos of the license plate of a vehicle on a public roadway nor maintaining and querying a database of ALPR photos constitute a warrantless 'search.'"[31] However, "state and federal courts have cautioned that the technology could run afoul of the Fourth Amendment moving forward … in light of technological advances."[32] In a 2024 analysis, the Congressional Research Service highlighted sustained tracking of a particular suspect through ALPR systems or potentially using ALPRs in concert with other surveillance tools as potentially triggering Fourth Amendment protections.[33]

---

[24] LAPPA, *supra* note 18.
[25] UTAH CODE ANN. § 41-6a-2005 (West 2025).
[26] *See* U.S. CONST. amend. IV.
[27] *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, INT'L ASS'N OF CHIEFS OF POLICE 13 (Sept. 2009), https://www.theiacp.org/sites/default/files/all/k-m/LPR_Privacy_Impact_Assessment.pdf.
[28] Catherine Crump et al., *You are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements*, AM. CIV. LIBERTIES UNION 7 (July 2013), https://www.aclu.org/sites/default/files/field_document/071613-aclu-alprreport-opt-v05.pdf.
[29] *Id*.
[30] *License Plate Reader (LPR) Systems: Use Cases*, INT'L ASS'N OF CHIEFS OF POLICE 12 (2024), https://www.theiacp.org/sites/default/files/LPRUseCases%202024.01.pdf.
[31] Schmidt v. City of Norfolk, No. 2:24-cv621, 2026 WL 207513, at *1 (E.D. Va. Jan. 27, 2026) (citing to Rinaldi v. Sylvester, No. 24-CV-272, 2025 WL 2682691, at *17 (S.D.N.Y. Sept. 19, 2025) for a list of such cases).
[32] Berris et al., *supra* note 7. *See also* Schmidt, 2026 WL 207513, at *2 (noting that "several federal judges, including another judge of this Court, have expressly cautioned that their rejection of a constitutional challenge to the use of ALPR technology should not be indiscriminately extended because, as the number and capabilities of ALPR cameras expand, the constitutional balancing could conceivably tip the other way").
[33] Berris et al., *supra* note 7, at 2.

Return to Table of Contents

Conversely, the Kentucky Supreme Court unanimously found that a defendant convicted of driving under the influence: (1) did not have a reasonable expectation of privacy in his license plate in connection with a police officer's gathering of information from the plate; (2) did not have a reasonable expectation of privacy in information that a police officer discovered after using a license plate reader on the defendant's vehicle; and (3) the officer, who discovered that the defendant has an outstanding warrant for his arrest through the use of a license plate reader, had reasonable suspicion to stop the vehicle.[34] Similarly, in the Massachusetts case of Commonwealth v. McCarthy, the defendant, Jason McCarthy, was arrested after an investigation by law enforcement, including the use of ALPR data to track Mr. McCarthy in connection with a drug distribution investigation.[35] The officers used both historical ALPR data and real-time alerts to assist in developing the evidence needed to ultimately arrest the defendant.[36] Ultimately, the Supreme Judicial Court of Massachusetts determined that, "while the defendant has a constitutionally protected expectation of privacy in the whole of his public movements … that interest is not invaded by the limited extent and use of ALPR data in this case."[37] Finally, the Court of Appeals of Virginia found that a lower court erred in ruling that a search warrant was required for law enforcement to access the city's ALPR system to verify a suspect's statement regarding his movements on a specific date.[38]

Currently in force state ALPR laws differ in their scope. Some laws apply only to law enforcement use of ALPR systems.[39] Some apply to ALPR system use by "governmental entities," a broader category that includes law enforcement but not to private sector entities.[40] A few states' laws cover both governmental entities and private entities.[41] As part of developing this Act, the drafters had to decide on the Act's scope. Because ALPR system use by private entities and individuals could have First Amendment freedom of speech implications, this Model Act does not attempt to regulate ALPR use by private entities or individuals but does include a provision related to the use by governmental entities of ALPR data held by private entities.

This Act establishes: (1) who can use ALPR systems; (2) how those authorized individuals and entities can use data captured by or derived from ALPRs; (3) elements that governmental entities using ALPR data must include in policies that they adopt; and (4) penalties for violations of this Act. The purpose of these provisions is to create a uniform law that states can use to regulate the use of ALPR and to attempt to forestall any potential Fourth Amendment violations by limiting the uses of ALPR data in the absence of a warrant.

[34] Traft v. Commonwealth of Kentucky, 539 S.W.3d 647, 649-650 (Feb. 15, 2018).
[35] Commonwealth v. McCarthy, 484 Mass. 493, 494 (Apr. 16, 2020).
[36] *Id*.
[37] *Id*.
[38] Commonwealth v. Church, No. 0737-25-1, slip op. at 4 (Va. App. Oct. 14, 2025).
[39] LAPPA, *supra* note 18, at 4-5.
[40] *Id*.
[41] *Id*.

Return to Table of Contents

SECTION III. DEFINITIONS.

[*States may already have definitions in place for some or all of the following listed terms. In such case, states are free to use the existing definitions in place of those listed below.*]

For purposes of this Act, unless the context clearly indicates otherwise, the words and phrases listed below have the meanings given to them in this section:

(a) Alert.—"Alert" means an alert from an automatic license plate recognition system that a license plate or vehicle matches a license plate or vehicle on the hot list or another database utilized by the system for comparison purposes;

(b) Audit trail.—"Audit trail" means all records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the:

(1) Date and time of access;

(2) License plate number or other data elements used to query the system;

(3) Specific purpose, as set forth in this Act, for accessing or querying the system, including the offense type for any criminal investigation;

(4) Associated call for service or case number, if any; and

(5) Username of the individual or individuals who accessed or queried the system;[42]

(c) Audit trail data.—"Audit trail data" means all forms of data collected or generated by an automatic license plate recognition system for purposes of producing an audit trail;[43]

(d) Authorized user.—"Authorized user" means an individual that is an employee, contractor, or other person hired by a governmental entity who has completed the training required by such entity and has been authorized by the entity to access automatic license plate recognition system data;

(e) Automatic license plate recognition system.—"Automatic license plate recognition system" or "system" means a system of one or more fixed, mobile, or portable high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data. This term does not include a traffic control photographic system or an open road tolling system unless such

[42] VA. CODE ANN. § 2.2-5517(A) (West 2025).
[43] VA. CODE ANN. § 2.2-5517(A) (West 2025).

Return to Table of Contents

systems are equipped with automatic license plate recognition system software;[44]

(f) Automatic license plate recognition system data.—"Automatic license plate recognition system data" or "system data" means data captured by or derived from an automatic license plate recognition system including, but not limited to, global positioning device coordinates of the system that took the photograph, date and time, photograph, license plate number, and any other data captured by or derived from the system;[45]

(g) De-identified.—"De-identified" means that personal identifying information has been removed or obscured, including through encryption, in such a way that minimizes the risk of unintended disclosure of the individual;

(h) Governmental entity.—"Governmental entity" means any office, agency, board, bureau, committee, department, advisory board, commission, or institution of higher education of the state or a political subdivision of the state that is funded or established by the state or a political subdivision of the state as well as an individual acting as an agent or on behalf of a governmental entity. A law enforcement agency is a governmental entity;[46]

(i) Hot list.—"Hot list" means a list or lists of vehicles of interest against which the automatic license plate recognition system compares to vehicles that are observed by the system. Authorized hot lists include, but are not limited to, the National Insurance Crime Bureau; the National Crime Information Center; the Federal Bureau of Investigation; America's Missing: Broadcast Emergency Response (AMBER) Alerts and any other existing or new alerts authorized by the legislature; Department of Homeland Security watch lists; and any custom alerts in the state that pertain solely to missing and endangered individuals, witness locations, burglaries, grand theft, drug trafficking, and violent crimes;[47]

(j) Law enforcement agency.—"Law enforcement agency" means:

(1) A federal, state, local, or tribal police department or sheriff's office that is situated in, part of, or administered by, this state or any political subdivision thereof;

(2) A private police department in [state] that is responsible for the prevention and

[44] *See* N.C. GEN. STAT. ANN. § 20-183.30 (West 2025), UTAH CODE ANN. § 41-6a-2002 (West 2025), and VA. CODE ANN. § 2.2-5517(A) (West 2025). *See also* S.B. 447, § 1(2), 126th Gen. Assemb, 1st Reg. Sess. (S.C. 2025).
[45] ALA. ADMIN. CODE 265-X-6-.02 (2025); ARK. CODE ANN. § 12-12-1802 (West 2025); GA. CODE ANN. § 35-1-22 (West 2025); and MD. CODE ANN. PUB. SAFETY § 3-509 (West 2025).
[46] Taken in part from ARK. CODE ANN. § 12-12-1802 (West 2025).
[47] S.B. 274, Reg. Sess. (Cal. 2025).

Return to Table of Contents

detection of crime and the enforcement of the penal, traffic, or highway laws of [state];

(3) A federal, state, or local prosecutor's office that is situated in, part of, or administered by this state or any political subdivision thereof;

(4) A police department at an institution of high education; or

(5) Any full-time or part-time, paid or volunteer, staff or employee of an entity identified in this subsection;[48]

(k) Missing and endangered person.—"Missing and endangered person" means an individual who has been identified as a missing or endangered individual by at least one of the following:

(1) The National Criminal Information Center;

(2) The National Center for Missing and Exploited Children;

(3) The Missing Children Information Clearinghouse;

(4) A [state] America's Missing: Broadcast Emergency Response (AMBER) alert;

(5) A [state alert related to a senior citizen, *e.g.*, "Blue Alert"];

(6) A [state alert related to a vulnerable adult, *e.g.*, individual with autism alert];

(7) Any substantially similar alert under the laws of another state or territory of the United States; or

(8) A "be on the lookout (BOLO)" bulletin issued by a law enforcement agency;[49]

(l) Personal identifying information.—"Personal identifying information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual and includes, but is not limited to, names, gender, race, dates of birth, photographs, addresses, social security numbers, driver's license numbers, and biometric data. "Personal identifying information" does not include a license plate number;[50]

(m) Private entity.—"Private entity" means an individual or entity or organization that is not classified as a state, local government, Indian tribe, or foreign public entity and includes

[48] *Model Relief from Collateral Consequences of Conviction Act*, LEGIS. ANALYSIS & PUB. POL'Y ASS'N 17 (July 2024), https://legislativeanalysis.org/model-relief-from-collateral-consequences-of-conviction-act/
[49] N.C. GEN. STAT. ANN. § 20-183.30 (West 2025).
[50] ALA. ADMIN. CODE 265-X-6-.02 (2025).

Return to Table of Contents

both nonprofit and for-profit businesses, landowners, leaseholders, and commercial businesses that are not governmental entities;[51]

(n) Query.—"Query" means a search of automatic license plate recognition system data based on information entered by the system user, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the system;[52]

(o) Secured area.—"Secured area" means an area enclosed by clear boundaries, to which access is limited and not open to the public, and entry is obtainable only through specific access-control points;[53]

(p) System data.—"System data" means all forms of data collected or generated by an automatic license plate recognition system, including, but not limited to, images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted;[54]

(q) System owner.—"System owner" means an individual or entity that owns or operates an automatic license plate recognition system, including law enforcement agencies and other governmental entities;[55] and

(r) Vendor.—"Vendor" means a business, company, corporation, or other nongovernmental entity that contracts with a governmental entity for the installation, use, or maintenance of an automatic license plate recognition system.[56]

Commentary

The terms defined in this section are primarily based on existing state laws. These terms may already be defined under individual state law in reference to other topics, and states are free to use those definitions in lieu of the definitions provided in this section. However, some of the definitions in this section may have been revised to better fit the needs and circumstances of this Act, and changes to such definitions may impact the effectiveness of the Act.

[51] *See* ARK. CODE ANN. § 12-12-1802 (West 2025) and *What is a Private Entity? A Comprehensive Legal Overview*, US LEGAL FORMS (accessed Feb. 23, 2026), https://legal-resources.uslegalforms.com/p/private-entity.
[52] VA. CODE ANN. § 2.2-5517(A) (West 2025).
[53] ARK. CODE ANN. § 12-12-1802 (West 2025) and UTAH CODE ANN. § 41-6a-2002 (West 2025).
[54] VA. CODE ANN. § 2.2-5517(A) (West 2025).
[55] *See* 625 ILL. COMP. STAT ANN. 5/2-130 (West 2025).
[56] VA. CODE ANN. § 2.2-5517(A) (West 2025).

Return to Table of Contents

This Act uses the term "automatic license plate recognition system," but, as pointed out in footnote 6, these systems are also known by a number of other terms. The drafters recommend using the term "automatic license plate recognition system" as used in this Act for the sake of consistency across states; however, states are free to use whichever term they prefer.

The definition of "personal identifying information" set forth in subsection (l) specifically excludes license plate numbers as publicly displaying a license plate is required by all 50 states for identification purposes and license plates are issued to a specific vehicle, not an individual.

As used in this Act, the term "private entity" includes both individuals and entities that are not associated with the government. It includes entities such as homeowners' associations, organizations that own and operate private parking lots, and convenience stores. "Secured area" includes exterior spaces enclosed by a fence through which individuals and vehicles may only obtain access through a gate or similar entry point.

SECTION IV. AUTHORIZED USES AND GENERAL PROVISIONS.

(a) In general.—Except as provided in subsection (b), it is unlawful for any governmental entity to use an automatic license plate recognition system.[57]

(b) Authorized uses.—An automatic license plate recognition system may be used:

(1) By a law enforcement agency for the comparison of system data held by a database created by a law enforcement agency; a vendor with which the agency has a contract; or a database held by an entity with which the agency has an executed memorandum of understanding or data sharing agreement pursuant to subsections (c) and (d) for the use of the data:

(A) As part of a criminal investigation into an alleged violation of federal or state law or any ordinance of any county, city, town, or other political subdivision of this state where there is a reasonable suspicion that a crime was committed;

(B) As part of an active investigation related to a missing or endangered person, including whether to issue an alert for such individual, or an individual associated with human trafficking; or

(C) To receive and respond to alerts;

(2) By a governmental entity for the purpose of enforcing motor [carrier/vehicle] laws;

(3) By the [department of transportation] at ports of entry and weigh stations;

[57] ARK. CODE ANN. § 12-12-1803 (West 2025); S.B. 447, 126th Leg. Sess. (S.C. 2025).

Return to Table of Contents

(4) By a governmental parking enforcement entity for the purpose of enforcing state and local parking laws;

(5) By the [state department of public safety and/or state department of transportation] or its agents to collect tolls and to provide for the efficient and safe movement of vehicles on state highways;

(6) By a [public transit district] for the purpose of assessing roadway or parking needs and conducting a travel pattern analysis;

(7) By an institution of higher education for research, statistical, or educational purposes, so long as the data collected is de-identified; and

(8) By any system user for the purpose of controlling access to a secured area.[58]

(c) Contractual authority.—A governmental entity may enter into a contract with a vendor for the purpose of installing, operating, using, or maintaining an automatic license plate recognition system, provided that:[59]

(1) The vendor certifies that:

(A) It will not sell, use, or share any system data or audit trail data gathered in the state, except as permitted by this Act;

(B) Its system can purge system data as required by this Act;

(C) Its system can create an audit trail and purge such audit trail data as required by this Act; and

(D) The system meets information security standards as established by [reference to state or federal law];[60] and

(2) The contract specifies that system data and audit trail data are the property of the governmental entity.[61]

(d) Data sharing agreements.—A governmental entity may enter into memoranda of understanding or data sharing agreements with any other governmental entity, including any federal governmental entity or law enforcement agency, for the purpose of sharing system data. Such data sharing agreements and memoranda of understanding shall

[58] The provisions in this subsection were taken from ARK. CODE ANN. § 12-12-1803 (West 2025), MONT. CODE ANN. § 46-5-117 (West 2025), UTAH CODE ANN. § 41-6a-2003 (West 2025), and VA. CODE ANN. § 2.2-5517 (West 2025).
[59] VA. CODE ANN. § 2.2-5517 (West 2025).
[60] *Id*.
[61] *Id*.

Return to Table of Contents

expressly provide that:

(1) System data may not be accessed or used except as provided in this Act; and

(2) The recipient of the data must comply with all data classification, preservation, destruction, and security requirements of this Act.[62]

(e) Data uploading and updates.—

(1) Automatic license plate recognition system data generated by or on behalf of a governmental entity shall be uploaded and stored [immediately after/within *n* minutes/hours of being] captured by a system camera.[63]

(2) The databases used by a system to provide alerts shall be updated every [24] hours if such updates are available or as soon as practicable after such updates become available.[64]

(f) Audit trails.—Automatic license plate recognition systems owned and operated by governmental entities shall include the capability to create an audit trail that includes the following information:

(1) The date and time that the system is queried;

(2) The license plate number or other data elements used to query the system;

(3) The username of the individual who accessed the system and, as applicable, the organization or entity with whom the individual is affiliated;

(4) The purpose or justification for accessing the system, including the case number, if applicable; and

(5) Any other information collected by the system related to a query.[65]

(g) Special use permit.—Subject to the provisions of subsection (h), a governmental entity shall obtain a special use permit from the [state department of transportation] prior to installing any part of an automatic license plate recognition system within the right-of-way of a road on the state highway system for the purpose of capturing system data from vehicles traveling on a state highway and such devices shall be removed upon request of the department.[66]

---

[62] MINN. STAT. ANN. § 13.824 (West 2025).
[63] GA. CODE ANN. § 35-1-22 (West 2025).
[64] N.C. GEN. STAT. ANN. § 20-183.32 (West 2025) and VA. CODE ANN. § 2.2-5517 (West 2025).
[65] CAL. CIV. CODE § 1798.90.52 (West 2025) and VA. CODE ANN. § 2.2-5517 (West 2025).
[66] FLA. STAT. ANN. § 316.0777 (West 2025) and UTAH CODE ANN. § 41-6a-2003 (West 2025).

Return to Table of Contents

(h) Prohibitions.—It is unlawful for a system user or vendor to use an automated license plate recognition system to query information related to vehicles associated with particular individuals on the basis of the content of lawfully protected speech.[67]

(i) Vehicle stops.—

(1) An alert from an automatic license plate recognition system does not, by itself, constitute reasonable suspicion as grounds for a law enforcement agency to stop a vehicle.

(2) Prior to stopping a vehicle based on an alert, a law enforcement agency shall:

(A) Develop independent reasonable suspicion for the stop; or

(B) Confirm that the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification.[68]

(j) Querying system data.—

(1) Policies adopted by governmental entities pursuant to Section VII shall specify that access to system data shall be limited to such entity's authorized personnel, and such entities shall implement controls to ensure that only individuals with appropriate training and clearance are able to retrieve system data.[69]

(2) All information necessary for the creation of an audit trail shall be entered by a system user in order to query system data.[70]

(3) A law enforcement agency shall not query or download system data unless authorized by this Act except that the law enforcement agency may download audit trail data for purposes of generating audit reports.

(k) Data breach.—If an automatic license plate recognition system owned or operated by a governmental entity is the subject of a data breach, or the governmental entity has reason to believe a breach occurred, the entity shall notify the [attorney general] within [30 days] of the breach or its reason to believe that a breach occurred and shall notify the public of the breach or possible breach by posting on the entity's public-facing website and on social media accounts operated by the governmental entity.

---

[67] VA. CODE ANN. § 2.2-5517 (West 2025).
[68] MONT. CODE ANN. § 46-5-117 (West 2025); N.H. REV. STAT. ANN. § 261:75-b (2025); VA. CODE ANN. § 2.2-5517 (West 2025); H.B. 528, 2025 Reg. Sess. (Miss. 2025); H.B. 5659 and S.B. 1013, 2025 Leg. Sess. (R.I. 2025); and S.B. 447, 126th Leg. Sess. (S.C. 2025).
[69] IDAHO CODE ANN. § 49-1432 (West 2025).
[70] VA. CODE ANN. § 2.2-5517 (West 2025).

Return to Table of Contents

(1) Notice to the [attorney general] shall include a synopsis of the events surrounding the breach, the number of individuals in the state who were or potentially have been affected by the breach, and any actions taken by the entity to prevent a future breach.[71]

(l) Public awareness.—Subject to the provisions of subsection (h), a governmental entity that uses an automatic license plate recognition system shall take measures, including by posting information on the governmental entity's public-facing website, via social media, and in print, to promote public awareness of the system prior to or coincident with system implementation.[72]

(m) Existing systems.—A governmental entity with an automatic license plate recognition system already in use on the effective date of this Act has [six months] from such date to satisfy the requirements of this Act.

Commentary

This section sets forth the individuals and entities authorized to access and use ALPR system data and includes law enforcement; governmental entities for specific purposes; and institutions of higher education for research, statistical, or educational purposes as long as the information is de-identified. The Model Act's drafters based most of the statutory language in this section on already enacted state statutes.

Subsection (c) permits governmental entities to enter into contracts with vendors for the purpose of installing, operating, using, or maintaining an ALPR system. It requires the vendor to certify that it will not sell or otherwise share system data and that it will abide by the provisions of this Act. Similarly, subsection (d) permits governmental entities to enter into data sharing agreements or memoranda of understanding for the purpose of sharing system data with other governmental entities. This is primarily intended for law enforcement agencies to permit them to, for example, enter into a memorandum of understanding with a federal law enforcement agency in order to access ALPR data held by that agency.

Subsection (e) requires that data obtained by ALPR cameras be uploaded within a certain amount of time. The drafters have not specified a time period but recommend that the data be uploaded either immediately or within a very few minutes in case the vehicle is the subject of a notification. This subsection also requires that the databases used to issue alerts be updated a minimum of every 24 hours.

Audit trails, as set forth in subsection (f), are intended to capture certain data related to ALPR system queries which can be used during internal audits required to be conducted by governmental entities pursuant to policies adopted by such entities pursuant to Section VII.

[71] FLA. CODE ANN. § 501.171 (West 2025).
[72] VA. CODE ANN. § 2.2-5517 (West 2025).

Return to Table of Contents

These audit trails can be used to, among other things, uncover unauthorized access to system data or unauthorized uses of system data.

Subsection (g) requires governmental entities to obtain a special use permit from the department of transportation, or similar agency or authority in the state, prior to installing an ALPR camera on agency or authority owned infrastructure on the right-of-way along a state highway. It also requires the entity to immediately remove such camera upon request of the department. The drafters anticipate that state legislators, in consultation with representatives from the respective agency or authority, may need to adjust this provision to account for state-specific nuances for special use permits.

Subsection (h) provides that ALPR system data cannot be used to infringe on an individual's civil rights. Finally, as with any other technology, ALPR systems may be the target of a data breach. Subsection (k) requires a governmental entity operating an ALPR system to notify the state attorney general of any such breach. A concomitant requirement to notify individuals whose license plate information may have been included in a data breach is not included because identifying those individuals might violate the federal Drivers Privacy Protection Act's prohibition against releasing information from motor vehicle records without the consent of the individual to whom the information pertains.[73]

SECTION V. DATA DESTRUCTION AND DATA PRESERVATION.

(a) In general.—Subject to the provisions of this section, governmental system users and vendors shall:

(1) Purge system data held by or on behalf of a governmental entity no later than [n] [days/months] from the date of its capture in such a manner that such data is destroyed and not recoverable by either the system user or the vendor; and

(2) Purge audit trail data held by or on behalf of a governmental entity no later than [two years] from the date of its capture in such a manner that such data is destroyed and not recoverable by either the system user or the vendor.[74]

(b) Data preservation.—Systems users and vendors shall preserve system data or audit trail data in the following circumstances:

(1) Upon the written request of:

(A) An investigating officer or law enforcement agency;

(B) The individual who is the subject of the investigation or prosecution; or

(C) An individual who is a party to a civil action in which a governmental entity is

[73] *See* 18 U.S.C.A. 2721 (2000).
[74] VA. CODE ANN. § 2.2-5517 (West 2025).

Return to Table of Contents

also a party;

(2) Upon the issuance of a state or federal search warrant;

(3) Upon the issuance of a subpoena or court order for the data;[75] or

(4) For the purpose of payment of a toll or penalty imposed under state highway tolls.

(c) Purging preserved data.—Systems users and vendors shall:

(1) Purge data preserved pursuant to subsections (b)(1) and (b)(2):

(A) When the investigation concludes without any criminal charges;

(B) When the statute of limitations expires and no criminal charges have been filed; or

(C) Upon a final disposition of any criminal or civil matter related to the data, including any direct appeals and any writs of habeas corpus pursuant to [reference to state law(s)] or federal law, in accordance with applicable records retention law and policy;[76]

(2) Purge data preserved pursuant to subsection (b)(3) upon a final disposition in the case which is the subject of the subpoena or court order or when the court that issued the subpoena or court order grants permission for the data to be purged; and

(3) Purge data preserved pursuant to subsection (b)(4) once such data is no longer needed for the collection of the toll or penalty imposed.

(d) Notice of request.—Subsection (b) does not apply to system data or audit trail data that the system user or vendor purged pursuant to subsection (a) before the system user or vendor received a written preservation request.

Commentary

One aspect common to all existing ALPR system laws is a provision governing how long system data can be maintained before it must be purged. As of September 2025, 23 states, the District of Columbia, and the U.S. Virgin Islands have statutes and/or rules in place that regulate the use of ALPRs.[77] However, there is no consensus among those jurisdictions as to how long system data can be maintained. Time periods range from three minutes in New Hampshire[78] to five years in Alabama,[79] with approximately half of the states with existing ALPR system laws

[75] MONT. CODE ANN. § 46-5-118 (West 2025) and NEB. REV. STAT. ANN. § 60-3204 (West 2025).
[76] MINN. CODE ANN. § 13.824 (West 2025).
[77] LAPPA, *supra* note 18 at 4.
[78] N.H. REV. STAT. ANN. § 261:75-b (2025).
[79] ALA. ADMIN. CODE r. 265-X-6-.06 (2025).

Return to Table of Contents

having retention periods of 90 days or less and the remaining half having retention periods of 150 days or more.[80]

This section also provides that certain individuals and entities are entitled to request that system data be preserved beyond the purge date for use in active criminal investigations, prosecutions, and civil actions. The data must then be purged upon the occurrence of one of the circumstances listed in this section, including the conclusion of a criminal investigation or the expiration of the statute of limitations without the filing of criminal charges.

SECTION VI. DATA DISCLOSURE.

(a) In general.—No governmental system user or vendor may sell, trade, exchange, share, or disclose any system data or audit trail data except as provided in this Act.[81] Images and data captured by an automatic license plate reader system not owned or operated by or on behalf of a governmental entity are not subject to this provision.

(b) Confidentiality.—System data and audit trail data are confidential and are not subject to disclosure under [reference to state freedom of information statute(s) and/or public records laws].

(c) Law enforcement.—Except as provided in subsection (e), a law enforcement agency may only share or disclose system data or audit trail data:

(1) With another law enforcement agency for purposes set forth in this Act, including law enforcement agencies in other states and federal law enforcement agencies, which may include allowing another law enforcement agency to query system data, provided that the agency receiving such data complies with all of the provisions of this Act;

(2) With the state attorney general, state or local prosecutors, and other attorneys representing the State of [state] in a criminal proceeding for purposes set forth in Section IV or for complying with discovery or a court order in a criminal proceeding;

(3) With a defendant or defendant's counsel for purposes of complying with discovery or a court order in a criminal proceeding;

(4) Pursuant to a court order or a subpoena duces tecum in any criminal or civil proceeding;

[80] Drabert, *supra* note 8.
[81] ARK. CODE ANN. § 12-12-1804 (West 2025).

Return to Table of Contents

(5) With the vendor for maintenance or quality assurance purposes;

(6) To alert the public to an emergency situation, a missing or endangered person, an individual associated with human trafficking, or an individual with an outstanding warrant; or

(7) To satisfy the reporting requirements of Section IX.[82]

(d) Other governmental entities.—Except as provided in subsection (e), a system user that is a non-law enforcement governmental entity may only share or disclose system data or audit trail data for the purposes identified in paragraphs (4), (5) and (7) of subsection (c).

(e) Other disclosures.—Individuals or entities conducting the [biennial] audit required pursuant to Section VIII shall have access to system data and audit trail data only as may be necessary for the limited purpose of conducting the audit.

(f) Private entity data.—A private entity may voluntarily share or otherwise provide access to system data with a law enforcement agency but may not be compelled to disclose system data or audit trail data absent a valid search warrant.[83]

(g) Aggregated data.—Notwithstanding [reference to applicable state record retention law(s)] or the provisions of this section, a governmental entity may share or disclose aggregated de-identified system data for research or statistical purposes.

(h) Vendor notification.—A vendor shall immediately notify the contracting system user upon receipt of a subpoena duces tecum, execution of a search warrant, or any other request from a third party for any system data or audit trail data, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

Commentary

This section prohibits vendors and system users, including law enforcement agencies, from selling, trading, exchanging, sharing, or disclosing ALPR system data for any purpose not expressly permitted by this Act. This provision only applies to systems owned and operated by or on behalf of a governmental entity. Subsection (b) provides that system data is confidential and not subject to public records or state freedom of information act laws.

Subsection (c), based on Virginia's law, delineates the circumstances under which a law enforcement entity may share or disclose system data and/or audit trail information. These circumstances include sharing data with another law enforcement agency for criminal investigation purposes or any other purpose permitted pursuant to the provisions of this Act.

[82] VA. CODE ANN. § 2.2-5517 (West 2025).
[83] UTAH CODE ANN. § 41-6a-2004 (West 2025).

Return to Table of Contents

Under subsection (e), it also permits entities that are conducting the biennial audit required by Section VIII to access system and audit trail data as necessary to perform duties related to the audit.

This section permits private entities to voluntarily share or otherwise provide access to ALPR system data acquired by the private entity with a law enforcement agency without the necessity of a search warrant; however, such entities cannot be compelled to disclose that data. In situations where a private entity refuses to share data with a law enforcement agency, the agency must obtain a search warrant to obtain the data.

SECTION VII. GOVERNMENTAL ENTITY POLICIES FOR USE.

(a) In general.—Prior to or coincident with using an automatic license plate recognition system, a governmental entity shall establish and enforce a policy governing the system's use that includes:

(1) A description of the job title or other designation of the employees and independent contractors who are authorized to query, access, use, or collect system data;[84]

(2) The databases used to compare data obtained by the system;[85]

(3) The purposes for which the system can be used or accessed;

(4) Prohibiting the download of system data that is not related to a purpose set forth in this Act, except for downloads of audit trail data for purposes of generating audit reports;

(5) An internal auditing procedure that occurs at least once every [30 days] including a review of audit trail reports;

(6) Procedures for system data and audit trail data destruction and preservation consistent with Section V;

(7) Restrictions on system data and audit trail data disclosure consistent with Section VI;

(8) Prohibiting the sale of system or audit trail data and restrictions on the sharing of system data and audit trail data consistent with this Act;

(9) Procedures to certify whether an automatic license plate recognition system experienced a data breach and a requirement for any vendor operating a database for a law enforcement agency to report any breaches of the database, the number of

[84] CAL. CIV. CODE §§ 1798.90.51 and 1798.90.53 (West 2025).
[85] N.C. GEN. STAT. ANN. § 20-183.31 (West 2025).

Return to Table of Contents

employees with access to the database, and any unauthorized releases of information;[86]

(10) Security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect the system, system data, and audit trail data from unauthorized access, destruction, use, modification, or disclosure;[87]

(11) Procedures for system maintenance and calibration and retaining records of such maintenance and calibration on file; and

(12) Mandatory training requirements for individuals who will use or access the system.[88]

(b) Law enforcement policy.—In addition to the requirements in subsection (a), a policy developed by a law enforcement agency must also include procedures:

(1) To ensure that the databases used by the system to generate the alerts set forth in Section IV are updated as required by this Act;

(2) To protect information collected and stored in an automatic license plate recognition system database;[89] and

(3) Consistent with Section IV to confirm the accuracy of any alerts made by the system before stopping a vehicle.

(c) Public posting.—Prior to or coincident with using an automatic license plate recognition system, it is recommended that a governmental entity post the policy developed pursuant to this section on its public-facing website.[90]

(d) Existing systems.—A governmental entity using an automatic license plate recognition system on the effective date of this Act has [six months] from such date to satisfy the requirements of this section.

Commentary

The IACP recommends that an agency's "purpose and objectives as well as the specific criteria for use … be clearly articulated in agency policy."[91] Following that recommendation, this section requires governmental entities using an ALPR system to adopt and implement policies related to accessing, using, and disclosing system data. It also includes additional

[86] MD. CODE ANN. PUB. SAFETY § 3-509 (West 2025).
[87] CAL. CIV. CODE § 1798.90.53 (West 2025).
[88] VA. CODE ANN. § 2.2-5517 (West 2025).
[89] MD. CODE ANN. PUB. SAFETY § 3-509 (West 2025).
[90] *Id*.
[91] IACP, *supra* note 30.

Return to Table of Contents

requirements for policies adopted by law enforcement agencies related to updating notifications generated by an ALPR system, procedures to protect information gathered by the system, and procedures to confirm the accuracy of information generated by a notification. The IACP also recommends that governmental entities "consider sharing their [ALPR] policy with the community—either by publishing the [ALPR] policy publicly or by simply communicating the policy goals and intentions of deploying the technology through other available communications channels (community meetings, social media, etc.),"[92] a recommendation encapsulated in subsection (c).

SECTION VIII. INDEPENDENT AUDITING AND REVIEW.

(a) In general.—A governmental entity that utilizes one or more automatic license plate recognition systems shall arrange for an [independent] [biennial] audit of each system to verify compliance with this Act, including an examination of how the data is used, access to the system, and whether data destruction occurs as required.[93]

(b) Audit results.—

(1) The results of the audit are public and shall be published on the public-facing website of the governmental entity that is the subject of the audit.

(2) A report summarizing the results of each audit shall be provided to the [state attorney general] and to the chairs and ranking minority members of the committees of the [house and senate/general assembly] with jurisdiction over data practices and public safety issues within 30 days following completion of the audit.[94]

(c) Audit review.—

(1) The [state attorney general] shall review the results of each audit.

(2) If the [state attorney general] determines that there is a pattern of substantial noncompliance with this Act by the governmental entity, he or she shall issue an order of suspension pursuant to subsection (c)(3) and shall immediately notify the governmental entity, and such entity shall immediately suspend operation of all systems until the [attorney general] authorizes the governmental entity to reinstate their use.

(3) The [state attorney general] may issue an order of suspension upon review of the results of the audit, review of the applicable provisions of this Act, and after

[92] *Id*.
[93] MINN. STAT. ANN. § 13.824 (West 2025).
[94] *Id*.

Return to Table of Contents

providing the governmental entity with a reasonable opportunity to respond to the audit's findings.

(4) An order of suspension must include the following information:

(A) The basis for the issuance of the order;

(B) The steps the entity must take to resume operation of the system; and

(C) Procedures to appeal the order of suspension.

Commentary

This section requires that governmental entities arrange for an audit of an ALPR system operated or used by the entity for the purpose of verifying compliance with this Act. Audits can be conducted by an independent outside entity or by the entity itself. Having an independent entity conduct the audit would alleviate any potential concerns about the accuracy of the audit; however, such audits might implicate privacy concerns and would also have a monetary cost that might be prohibitive for local governmental entities.

System audits can identify unauthorized access to system data, unauthorized disclosures, maintaining data longer than permitted by the Act, and inaccuracies in system notifications. Audit results are subject to public records laws and must be published on the entity's website. A copy of the audit results must be sent to the attorney general, or another individual or entity selected by a state, for review. If the attorney general finds that there has been a pattern of noncompliance with the Act, the attorney general must issue an order of suspension that includes the information required by paragraph (4) and notify the entity that it must cease operating an ALPR system until authority to reinstate the use of the system is authorized by the attorney general. The governmental entity must be given a reasonable opportunity to respond to the audit's findings, and the order of suspension must include procedures that the entity can take to appeal the order of suspension.

SECTION IX. REPORTING BY GOVERNMENTAL ENTITIES.

(a) Law enforcement.—

(1) A law enforcement agency that uses an automatic license plate recognition system shall report to the [state department of police] by [April 1] of each year, in a format to be determined by the [state department of police] on its use of the system during the preceding calendar year, which shall include the following data, if available:

(A) The total number of cameras owned or leased by the agency as part of a system at the conclusion of each calendar year, including the number of fixed cameras, mobile cameras, and portable cameras;

(B) A list of the current and previous locations, including dates at those locations, of any fixed system or other surveillance devices with automated license plate

reader capability used by the agency;

(C) A list of all state and federal databases with which the system data was compared, unless the existence of any such database itself is not public information;

(D) The number of system readings being retained on the system database;[95]

(E) The number of requests to preserve data received by the agency and the purpose of each request;

(F) The total number of times the system was queried, including the specific purposes of the queries, and the offense types for any criminal investigations;

(G) The total number of alerts generated by the system and the number of those alerts that resulted in an enforcement action;[96]

(H) The number of motor vehicles stopped based on alerts from the system, including the specific reasons for the alerts;

(I) Whether the agency allows any other law enforcement agencies to access its system data, and if so, which other agencies have been granted such access;

(J) The number of requests made to the agency for system data, including specific numbers for the number of:

(i) Requests that resulted in a release of information;

(ii) Out-of-state requests and those that resulted in a release of information; and

(iii)Federal requests and the number that resulted in a release of information;[97]

(K) The number of identified instances of unauthorized use of or access to the system, including the nature and circumstances of each such instance, the steps taken to prevent future instances of unauthorized use or access, and any disciplinary action taken against the individual who engaged in unauthorized use of or access to the system;

(L) Any data breaches and steps taken to protect system data as a result of such

[95] MD. CODE ANN. PUB. SAFETY § 3-509 (West 2025).
[96] VT. STAT. ANN. tit. 23, § 1607 (West 2025).
[97] MD. CODE ANN. PUB. SAFETY § 3-509 (West 2025).

Return to Table of Contents

breach;

(M) The number of subpoenas duces tecum, search warrants, court orders, and any other requests received from a third party for system data or audit trail data, including the identity of the individual or entity that requested the issuance of such subpoena duces tecum or court order, executed such search warrant, or requested such data, and whether any data was provided pursuant to such subpoena, search warrant, court order, or other request, unless disclosure is otherwise prohibited by law;

(N) The number of search warrants issued for system data held by a private entity, the purposes for which such data was requested, and the number of arrests made and/or criminal charges filed as a result of such data;

(O) A list of audits completed pursuant to Section VIII; and

(P) The total annualized fixed and variable costs associated with the operation of all systems used by law enforcement agencies and an estimate of the total of such costs per unit.[98]

(2) The [state department of police] shall aggregate the data provided pursuant to paragraph (1) and report it to the governor, the [legislature], and [any other appropriate commission or other entity, such as a state crime commission] by [July 1] of each year.

(b) Other governmental entities.—

(1) A governmental entity that is not a law enforcement agency that uses an automatic license plate recognition system shall report to the [state department of transportation] by [April 1] of each year, in a format to be determined by the [department of transportation] on its use of the system during the preceding calendar year, which shall include the information specified in clauses (A), (B), (C), (D), (E), (F), (I), (K), (L), (M), and (O) of subsection (a)(1).

(2) The [state department of transportation] shall aggregate the data provided pursuant to subsection (b)(1) and report it to the governor, the [state legislature], and [any other appropriate commission or other entity, such as a state crime commission] by

[98] VT. STAT. ANN. tit. 23, § 1607 (West 2025) and VA. CODE ANN. § 2.2-5517 (West 2025).

Return to Table of Contents

[July 1] of each year.

(c) Public posting.—Governmental entities shall post the reports prepared pursuant to this section on its public-facing website except that the governmental entity shall remove or de-identify any data that:

(1) Contains personal or case identifying information;

(2) Contains an articulable concern for any individual's safety;

(3) Is otherwise prohibited from public disclosure by federal or state statute; or

(4) May compromise sensitive criminal justice information if disclosed.[99]

Commentary

The reporting requirements detailed in this section are intended to provide information regarding ALPR systems owned and operated by governmental entities using such systems in the state. Reporting requirements are a component of state ALPR system laws in 11 states, which include states with laws applicable only to law enforcement agencies[100] and states with laws applicable to other entities in addition to law enforcement.[101] A working group member emphasized that some of the information required to be reported by law enforcement entities in subsection (a)(1) may be difficult to track and/or report depending on the size of the jurisdiction served by the ALPR system and vendor system agreements. Therefore, the drafters have specified that such information should be reported if it is available.

Throughout this Act, the drafters treat ALPR systems users that are law enforcement agencies and non-law enforcement governmental entities similarly in some respects and differently in others. Reporting requirements are one area where the drafters concluded that different treatment makes sense. Accordingly, law enforcement agencies must report all information identified in subsection (a). Non-law enforcement governmental entities have fewer reporting requirements, as subsection (b) eliminates some reporting categories specific to law enforcement activity. Because ALPR use by private entities is outside the scope of this Act, the Model Act does not place reporting requirements on private entity ALPR system users. As of August 2025, Arkansas is the only state that requires private entity ALPR system users to report data (albeit in limited fashion).[102]

The drafters suggested April 1 as the date when reports from law enforcement and other governmental entities should be submitted and July 1 as the date for aggregated reports to the governor and state legislature based on Virginia's law. States are, of course, free to choose any date they wish; however, the drafters recommend that there be a period of at least 30 days between the two dates to allow time for the information to be aggregated and put to form for submission to the governor and legislature pursuant to subsections (a)(2) and (b)(2).

[99] VA. CODE ANN. § 2.2-5517 (West 2025).
[100] LAPPA, *supra* note 18 at 4-8.
[101] *Id*.
[102] ARK. CODE ANN. § 12-12-1805 (West 2025).

Return to Table of Contents

SECTION X. CIVIL AND CRIMINAL PENALTIES; USE AS EVIDENCE.

(a) In general.—Any governmental system user, vendor, or other individual or entity who knowingly and willfully requests, uses, obtains, or attempts to obtain under false pretenses or for any purpose other than one authorized by this Act, or otherwise violates any provision of this Act, is guilty of a [class] misdemeanor.[103]

(b) Inadmissible evidence.—If system data was obtained in violation of this Act or if the use of such data would be a violation of this Act, such data may not be received in evidence in any trial, hearing, or other proceeding before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of [state].[104]

(c) Civil action.—In addition to any other sanctions, penalties, or remedies provided by state or federal law, an individual harmed by a violation of this Act including, but not limited to, unauthorized access, use, or sharing of system data or a breach of security of a system, may bring a civil action in any court of competent jurisdiction against an individual or entity that knowingly caused the harm. The court may award a combination of any one or more of the following:

(1) Actual damages, but not less than liquidated damages in the amount of [$];

(2) Punitive damages upon proof of willful or reckless disregard of the law;

(3) Reasonable attorney's fees and other litigation costs reasonably incurred; and

(4) Other preliminary and equitable relief as the court determines to be appropriate.[105]

Commentary

This section provides civil and criminal penalties may be imposed against an individual or entity who has violated any provision of this Act. The California law on which subsection (c)(1) is based recommends liquidated damages in the amount of $2,500. States can choose any dollar amount they wish; however, the amount should be sufficient to deter the behavior that is the cause of the damages.

[103] GA. CODE ANN. § 35-1-22 (West 2025) and VA CODE ANN. § 2.2-5517 (West 2025).
[104] ARK. CODE ANN. § 12-12-1806 (West 2025).
[105] CAL. CIV. CODE § 1798.90.54 (West 2025).

Return to Table of Contents

SECTION XI. FUNDING.

(a) In general.— The [legislature] shall appropriate [$ _____] to the [relevant governmental entities] to assist governmental entities subject to the requirements of Section IX in meeting the reporting requirements of that section.

(b) Federal funds.—Governmental entities may pursue federal funding, matching funds, grants, and foundation funding for the purpose of purchasing automatic license plate recognition system equipment and any ongoing costs associated with operating a system.

(c) Receipt of funding.—Governmental entities may receive such gifts, grants, and endowments from public or private sources as may be made from time to time, for the use and benefit of the purposes of this Act and expend the same, or any income derived from it, according to the terms of the gifts, grants, or endowments.

Commentary

Because this Act does not require any governmental entities to own and operate ALPR systems, this section does not provide state funding for the purchase of ALPR system equipment or the ongoing costs of operating an ALPR system. The section does, however, provide for appropriations to governmental entities for the purpose of costs associated with the reporting requirements in Section IX. It also provides statutory authorization for governmental entities to: (1) pursue and receive federal or state grants for the purpose of purchasing ALPR system equipment and any ongoing costs associated with operating an ALPR system; and (2) receive gifts, grants, and other endowments to offset the costs of operating an ALPR system.

Some additional sources of funding that governmental entities might consider applying for include general state and federal law enforcement grants and grants through the Edward Byrne Memorial Justice Assistance Grant (JAG) Program (Bureau of Justice Assistance).[106] The JAG program is a leading source of federal justice funding to state and local jurisdictions and provides states, tribes, and local governments with critical funding necessary to support a range of program areas, including law enforcement, prosecution, crime prevention, corrections and community corrections, drug treatment and enforcement, planning, evaluation, technology improvement, and related law enforcement and corrections programs.[107]

[106] *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program*, CONGRESS.GOV (April 4, 2025), https://www.congress.gov/crs-product/IF10691.
[107] *Id*.

Return to Table of Contents

SECTION XII. RULES AND REGULATIONS.

Unless specified differently in this Act, within [six (6) months] of the effective date of this Act, the [state department of police and/or other appropriate governmental entities] shall initiate a rulemaking to promulgate such rules and regulations as are necessary to implement this Act.

Commentary

The drafters recommend that the governmental entity charged with developing the operational plan referenced in Section VII should also be the entity that promulgates rules and regulations necessary to implement this Act. However, consideration of issues related to data retention and privacy concerns may necessitate other governmental entities' inclusion in creating rules related to this Act.

SECTION XIII. SEVERABILITY.

If any provision of this Act or application thereof to any individual or circumstance is held invalid, the remaining provisions of this Act shall not be affected nor diminished.

SECTION XIV. EFFECTIVE DATE.

This Act shall be effective on [specific date or reference to standard state method of determination of the effect].

Return to Table of Contents

ABOUT THE LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION

The Legislative Analysis and Public Policy Association (LAPPA) is a 501(c)(3) nonprofit organization whose mission is to conduct legal and legislative research and analysis and draft legislation on effective law and policy in the areas of public safety and health, substance use disorders, and the criminal justice system.

LAPPA produces up-to-the-minute comparative analyses, publications, educational brochures, and other tools ranging from podcasts to model laws and policies that can be used by national, state, and local criminal justice and substance use disorder practitioners who want the latest comprehensive information on law and policy. Examples of topics on which LAPPA has assisted stakeholders include naloxone laws, law enforcement/community engagement, alternatives to incarceration for those with substance use disorders, medication for addiction treatment in correctional settings, and the involuntary commitment and guardianship of individuals with alcohol or substance use disorders.

For more information about LAPPA, please visit: https://legislativeanalysis.org/.


LAPPA
LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION