MODEL STATUTE AUTHORIZING AND REGULATING THE USE OF AUTOMATED LICENSE PLATE READERS

I. DEFINITIONS

(A) **"Automated License Plate Readers"** or **"ALPRs"** means any device that automatically captures license plate images and detects license plate characters, including any camera that is used in conjunction with software that detects license plate characters.

(B) "**ALPR Data**" means any data that is captured or extracted by ALPRs, including but not limited to license plate characters, vehicle attributes, images, videos, and metadata.

(C) "**Hotlist"** means any list of license plates used in conjunction with an ALPR to generate an alert when a particular plate has been detected.

(D) **"Historical Data"** means any ALPR data that has been stored for later access.

(E) "**Governmental Agency"** or **"Agency"** means any state or local governmental agency, organization, department, or entity, and the employees or agents thereof.

(F) **"Encrypted"** means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

II. DEMOCRATIC AUTHORIZATION

(A) The State Police shall be authorized to use ALPRs and ALPR data for investigative purposes, as set forth in Section III(B), in accordance with the terms of this Act.

(B) State agencies shall be authorized to use ALPRs and ALPR data for non-investigative purposes, as set forth in Section III(A), in accordance with the terms of this Act.

(C) Each local government shall have the power to adopt and amend local laws, consistent with the terms of this Act, authorizing and regulating the use of ALPRs and ALPR data or prohibiting such use by agencies within their jurisdiction, after an opportunity for public comment at a regularly scheduled meeting of the local government's legislative body. Any use of ALPRs or ALPR data by a local government agency shall be governed by this Act.

(D) No governmental agency shall use ALPRs or ALPR data absent express legislative authorization as set forth in this Section.

Editor's note. *The purpose of this Section is to ensure that government agencies use ALPRs only pursuant to legislative authorization. Legislative bodies are well-suited to weigh the competing costs and benefits of policing technologies and to institute appropriate safeguards. See United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring). Subsection (C), modeled after state home rule statutes, enables local governments to authorize ALPR use through the legislative process after an opportunity for public comment. Cf. Cal. Civ. Code § 1798.90.55(a) (requiring public comment period before ALPR deployment).*

III. AUTHORIZED PURPOSES

(A) **Non-investigative purposes.** Agencies may use ALPRs and ALPR data for the following non-investigative purposes:

(i) Performing weigh station duties;

(ii) monitoring or maintaining an agency's own vehicles or equipment;

(iii) assisting in the control of access to a secured area;

(iv) collecting electronic tolls; or

(v) complying with the provisions of this Act.

(B) **Investigative purposes.** Agencies may use ALPR hotlists and access ALPR historical data for the following investigative purposes:

(i) Pursuing information relevant to an ongoing criminal investigation of a felony, violent crime, or terrorist act;

(ii) Apprehending an individual with an outstanding felony warrant;

(iii) Locating a missing or endangered person; or

(iv) Locating a lost or stolen vehicle.

(C) Agencies are prohibited from using ALPRs or ALPR data for the purpose of identifying individuals engaged in lawful First Amendment activities, such as protests, participation in a noncriminal organization, or religious services.

(D) Government agencies shall not use ALPRs or ALPR data for any purpose not expressly authorized in this Section.

Editor's note. *Specifying authorized purposes can help to ensure that ALPRs are used only when their benefits outweigh their costs. For example, ALPR use may be justified when the expected benefits are particularly large (e.g., use of ALPR to investigate terrorism and serious criminal offenses) or the expected harms are relatively small (e.g., use of ALPR in a secured non-public area). Cf. Mont. Code § 46-5-117(2)(d)(v) (authorizing use for, inter alia, investigation of a "homicide, shooting, or other major crime or incident"); N.H. Rev. Stat. § 261:75-(b)(V) (same); Cal. Civil Code §§ 7284.6, 1798.90.55 (prohibiting the sharing of ALPR data with federal immigration agencies). The investigative purposes listed above are intended only as a starting point. Depending on the state, these purposes may need to be narrowed — for example, because a state has classified some minor offenses as felonies. States may wish to authorize local governments to enact legislation adding or removing offenses to the list — this would enable localities to tailor their ALPR use to local enforcement priorities.*

IV. AUTHORIZED USES

In furtherance of an authorized investigative purpose set forth in Section III(B), a law enforcement agency may use ALPRs and ALPR data in the following ways:

(A) **Generating hotlist alerts.** An agency may use an ALPR to compare scanned license plates against a hotlist and to generate an alert if the ALPR detects a match.

(i) An agency shall update all hotlists

(a) on a daily basis; and

(b) when new bulletins are issued or cancelled.

(ii) Prior to stopping a vehicle on the basis of a hotlist alert, a law enforcement officer shall confirm,

(a) that the license plate on the vehicle matches the license plate displayed on the ALPR; and

(b) that the hotlist alert relates to an authorized purpose, as set forth in Section III of this Act.

The officer's confirmation shall be recorded in the agency's audit log.

(iii) If an alerted offense is associated with the registered owner of the vehicle, rather than the vehicle itself, officers shall make reasonable efforts to ascertain whether the driver matches the description of the registered owner prior to taking enforcement action, absent exigent circumstances.

(iv) An agency shall not use any hotlist that includes plates or vehicles sought for any purpose other than those specified in Section III(B) of this Act.

Editor's note. *The purpose of Subsection (A) is to minimize the risk that error, human or technological, will result in unwarranted vehicle stops. See Mont. Code § 46-5-117(vi), (vii) (hotlists must be updated daily and officers must confirm, prior to stopping a vehicle (a) that the vehicle's license plate matches the ALPR read and (b) that the hotlist alert relates to an authorized purpose); N.H. Rev. Stat. § 261:75-b(IV), (VI) (same).*

(B) Use of historical data to identify a vehicle in furtherance of an authorized investigative purpose. An agency may access the historical data of any ALPR located within a 0.5 square mile radius of a crime scene to identify vehicles of interest related to that crime.

(i) Additionally, an agency may, for the purpose of identifying a vehicle of interest related to a crime, access the historical data of any ALPR for which there is reasonable suspicion that the ALPR captured data regarding the vehicle of interest.

(ii) An officer accessing historical ALPR data under this Subsection shall create a record in the audit trail identifying:

(a) the name of the officer accessing the data;

(b) the date, time, and location of the crime scene or incident;

(c) the case number and reason for accessing the ALPR data; and

(d) the location of the ALPR accessed.

Editor's note. *Historical data, once collected, can be used in various ways. Legislatures should consider authorizing specified use cases for historical data and tailoring safeguards to those use cases, rather than creating a blanket authorization for the use of historical data in general. Subsections B, C, and D address use of historical data to identify a vehicle, determine the location of a known vehicle, and track the movements of a vehicle, respectively.*

(C) Use of historical data to determine the location of a known vehicle in furtherance of an authorized investigative purpose.

(i) An agency may search recent historical data, no older than six hours, provided there is a reasonable basis to believe such data would assist in effectuating an arrest, rendering aid to a missing or endangered person, or recovering a lost or stolen vehicle.

(ii) An agency may search historical data collected within six hours before or after the commission of an offense listed in Section III(B)(i) of this Act to ascertain whether a vehicle was at or near the scene of the crime.

(iii) Any other use of historical data to determine the location of a known vehicle shall be governed by Subsection IV(D) of this Act.

(iv) An officer accessing historical ALPR data under this Subsection shall create a record in the audit trail identifying:

(a) the name of the officer accessing the data;
(b) the date, time, and location of the crime scene or incident;
(c) the case number and reason for accessing the ALPR data; and
(d) the location of the ALPR accessed.

(D) Use of historical data to track the movements of a vehicle in furtherance of an authorized investigative purpose.

(i) An agency may access historical data to track the movements of a vehicle only in the following circumstances:

(a) upon issuance of a warrant by a court of competent jurisdiction authorizing such access based upon probable cause that the data is relevant and material to an ongoing criminal investigation; or
(b) where officers have probable cause that the data is relevant and material to an ongoing criminal investigation and exigent circumstances justify accessing the data without first obtaining a warrant.

(ii) An officer accessing stored ALPR data under this Subsection shall create a record in the audit trail identifying:

(a) the name of the officer accessing the data;
(b) if a warrant has been issued, the temporal and geographic scope of the warrant;
(c) if a warrant has not been issued, the nature of the exigent circumstances;
(d) all search queries performed; and
(e) all ALPR data accessed.

Editor's note. *Data about individuals' locations and movements over time can reveal a wealth of personal information. As the Supreme Court has observed in the context of GPS and cell-phone tracking, location data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (cleaned up). States have used different methods to address these privacy concerns. Minnesota's statute requires agencies to obtain a warrant before conducting location tracking through ALPR data. See Minn. Stat. § 13.824(2)(d). New Hampshire's statute functionally prohibits the collection of historical data, unless the data relates to a wanted person or vehicle. See N.H. Rev. Stat. § 261:75-b(VIII).*

(E) Data analytics and other uses.

(i) Governmental agencies may use ALPR data for purposes of analyzing traffic patterns.

(ii) Governmental agencies shall not use ALPRs or ALPR data for investigative purposes in any way not expressly authorized in this section.

Editor's note. *Increasingly, software tools allow agencies to conduct sophisticated analyses of ALPR data*

— from forming predictions about associations between individuals based on their driving patterns to detecting anomalous behavior such as "casing activity." As new use cases for ALPRs and ALPR data emerge, each should be considered on its own merits. This is especially important in the context of "software as a service" models, in which customers purchase software as a subscription and automatically receive new upgrades and features. In this way, an ALPR authorized by a legislature today may have a significantly different set of features in the future.

V. TREATMENT OF HISTORICAL DATA

(A) ALPRs authorized for use under this Act may store only the following types of data:

(i) license plate characters and issuing state;
(ii) color, make, model, and other characteristics of a vehicle; and
(iii) the time, data, and location of the license plate capture.

Editor's note. *In addition to detecting license plate characters and generating metadata, some ALPR systems can be configured to record video and still images, detect pedestrians and non-motorized vehicles, and collect data such as a vehicle's color, make, model, or speed of travel. Legislators should specify the specific types of data that may be collected in light of the purposes for which ALPRs may be used. See, e.g., Minn. Stat. § 13.824(2) (authorizing collection of license plate numbers, time and location data, and associated imagery); N.H. Rev. Stat. § 261:75-b(I) (prohibiting the collection of images depicting the occupants of a vehicle).*

(B) Retention of historical data.

(i) An agency shall permanently destroy ALPR data no later than thirty days after it is collected, unless such data:
  (a) is evidence that is stored in a casefile; or
  (b) is retained solely to fulfill the auditing and reporting requirements of this Act.

(ii) An agency may transfer ALPR data to the State Attorney General or designee within thirty days of its collection. The State Attorney General or designee shall securely store such data for a period of one year and ensure that it is not accessed, used, or transferred in any way, except as provided in Section V(B)(iii) of this Act.

(iii) An agency that seeks to access ALPR data in the possession of the State Attorney General or designee shall apply for a warrant authorizing such access in a court of competent jurisdiction. The court shall issue the warrant upon the applicant's showing of probable cause that the requested data is relevant and material to an ongoing criminal investigation.

Editor's note. *The purpose of a retention period is to limit an agency's access to historical data. The appropriate retention period will depend on various considerations, including the investigative value of retaining long-term data and the existence (or lack thereof) of alternative mechanisms to regulate agency access to ALPR data, such as a warrant requirement. In any event, in states with ALPR statutes, retention periods vary widely. Compare N.H. Rev. Stat. § 261:75-b(VIII) (three minutes), with Ark. Code § 12-12-1804(a) (150 days). The Model Act sets the retention period at thirty days, with an option for agencies to transfer data to the State Attorney General for longer-term storage. Some states may not be equipped to handle a high volume of retention requests; in this event, legislators might consider designating a county agency to store ALPR data.*

VI. ALPR DATA SHARING

(A) Except as otherwise provided in this Act, agencies shall not share, sell, or transmit retained ALPR data.

(i) Nothing in this Act shall be construed to supersede prosecutors' disclosure and discovery obligations to criminal defendants.

(ii) Any data request or data-sharing agreement authorized under this Act shall be submitted in electronic form and recorded in the agency's audit log.

(B) A regulatory entity, regulatory defendant, or criminal defendant seeking ALPR data in the possession of an agency or the State Attorney General or designee may apply for a court order for the disclosure of such data.

(i) A court of competent jurisdiction shall issue a court order requiring the disclosure of ALPR data if the applicant offers specific and articulable facts establishing reasonable grounds to believe that the captured plate data is relevant and material to the regulatory or criminal proceedings.

(ii) Pending issuance of such order, an agency shall preserve captured plate data upon a request from the applicant identifying:

(a) the cameras for which captured plate data shall be preserved;

(b) the license plate for which captured plate data shall be preserved; or

(c) the dates and times for which captured plate data shall be preserved.

Editor's note. *See Utah Code. 1953 § 41-6a-2005.*

(C) A law enforcement agency may share ALPR data generated by the agency's own ALPR with other law enforcement agencies in response to a written request for such data.

(i) Prior to such sharing, both agencies shall enter into a publicly-available data-sharing agreement. Such agreement shall provide that:

(a) with respect to the use of the data to be shared, the requesting agency must comply with the requirements of this Act and any other policies or regulations applicable to the agency sharing the data, including restrictions on retention and use;

(b) if, with respect to the use of any data shared, the requesting agency violates the requirements of this Act or any other policies or regulations applicable to the agency sharing the data, all sharing of ALPR data between the agencies shall immediately cease; and

(c) a record of any data shared shall be recorded in the audit logs of both agencies.

(ii) Except as provided in Section VI(C)(iii) of this Act, an agency may only share data that is relevant and material to a specific criminal case under investigation by the requesting agency. Agencies shall not share or receive ALPR data on an ongoing basis or share or receive data with any privately-owned or operated database or service.

(iii)An agency may share ALPR data on an ongoing basis with any local agency whose jurisdiction overlaps, is adjacent to, or is within a fifty mile radius of the sharing agency, subject to the requirements of Section VI(C)(i) of this Act.

Editor's note. *Interagency data sharing can undermine accountability, especially when the public and policymakers lack information about which agencies are accessing data and what policies govern data use. This Subsection seeks to bridge this information gap and ensure that consistent policies govern the use of ALPR data across agencies. Cf. Minn. Stat. §§ 13.824(2)(c), (4)(b) (prohibiting a centralized repository for ALPR data and requiring agencies receiving shared ALPR data to comply with the state's ALPR regulations).*

(D) An agency may share ALPR data with persons or entities for research and auditing purposes or in response to Freedom of Information Law requests. All ALPR data shared for such purposes must be in an anonymized and aggregate form, and devoid of any personally identifying information.

Editor's note. *Although some states prohibit the sharing of data in response to public records requests, see Okla. Stat. § 7-606.1(F)(2); Md. Pub. Safety Code § 3-509(d), Subsection (D) clarifies that data may be shared in response to public records requests in aggregated and anonymized form.*

(E) Any provision of this Act relating to an agency's use of ALPRs or ALPR data shall apply to the agency's use of any ALPR or ALPR data that has been shared with the agency in any manner.

VII. AGENCY PROCEDURES

(A) **ALPR Custodian.** An agency that uses an ALPR or ALPR data shall designate an ALPR Custodian, who shall be the administrator of the ALPR system and shall be responsible for:

(i) developing and publicizing a usage and privacy policy;

(ii) maintaining a list of the name and job title of all users who are authorized to use or access ALPR data;

(iii) developing training requirements; and

(iv) promptly disclosing to the public any security breach with respect to the agency's ALPRs or ALPR data.

(B) **Usage & Privacy Policy.** Agencies shall adopt and publicize a written ALPR usage and privacy policy prior to using or acquiring an ALPR or ALPR data. The policy shall conform to the requirements of this Act and shall include:

(i) the authorized uses for ALPRs and ALPR data;

(ii) a nondiscrimination provision prohibiting the deployment or use of ALPR or ALPR data solely on the basis of a protected characteristic;

(iii) policies in accordance with the terms of this Act governing data access, security, sharing, and retention;

(iv) training, auditing, and reporting requirements; and

(ii) a requirement that ALPR data be encrypted and secured against unauthorized access.

Editor's note. *See N.C. Gen. Stat. § 20-183.31(a); Cal. Civ. Code § 1798.90.53; Mont. Code § 46-5-117(d)(i); Md. Pub. Safety Code § 3-509(c)(1).*

(C) Audit trails. Each agency shall maintain audit trails of any ALPR or ALPR data use, including:

(i) a record of each hotlist alert and the reasons for each alert;

(ii) a record of each search of historical data, including:

(i) the date and time;

(ii) the name of the officer conducting the search;

(iii) the specific search queries;

(iv) the case number;

(v) a case narrative describing the offense under investigation and, for each search query, the specific reason the search is being conducted for those locations and dates/times; and

(vi) any ALPR data accessed;

(iii) a record of all requests for ALPR data, including the request, the requesting agency, and the purpose of the request; and

(iv) a record of all ALPR data shared and requests for ALPR data; and

(v) for any vehicle stop conducted on the basis of a hotlist alert, a record of the officer's confirmation that the license plate on the vehicle matches the license plate displayed on the ALPR and that the hotlist alert relates to an authorized purpose, as set forth in Section III of this Act.

Editor's note. *California's statute requires audit trails to include the reasons for searches of historical data, enabling better oversight. Cal. Civ. Code § 1798.90.52(a)(4). Some ALPR users, however, enter generic filler text (such as "investigation") when conducting searches. The Model Act requires ALPR users to enter case narratives with specific information about the reasons for their searches. The Model Act also requires agencies to publish certain aggregated data about their ALPR use (see Subsection (D)), akin to Minnesota's requirement that audit trails be made public except where they contain classified information. Minn. Stat. § 13.824(7)(b).*

(D) Public log. An agency that uses an ALPR or ALPR data shall compile and publish the following information quarterly on the agency's public website in an accessible and machine-readable format, viewable to the public:

(i) the aggregate number of searches of historical data and the reasons for the searches;

(ii) the number and type (stationary or mobile) of ALPRs owned or operated by the agency;

(iii) the location of each stationary ALPR;

(iv) a description of each hotlist used in the previous month;

(v) the total number of hotlist alerts and the number and type of enforcement actions resulting from hotlist alerts;

(vi) a list of all entities with whom the agency has shared ALPR data;

(vii) any data breaches or unauthorized uses of ALPRs, ALPR systems, or ALPR data.

Editor's note. *Although some agencies do not publicly disclose the locations of their ALPRs, doing so is essential for identifying and assessing disparities (racial, socioeconomic, or otherwise) in ALPR deployment. The Model Act requires agencies to disclose the general location of stationary ALPRs, which could be accomplished through a heat map or other data visualization.*

VIII. AUDITING

(A) The State Attorney General or designee shall audit each agency that uses an ALPR or ALPR data annually for compliance with the provisions of this Act.

(B) An agency that is being audited shall provide to the State Attorney General or designee access to any ALPR device, any ALPR data, any system for accessing ALPR data, and any records of ALPR or ALPR data use.

(C) The State Attorney General shall issue a public report with the results of each audit.

(D) If the State Attorney General determines that there is a pattern of substantial noncompliance with this Act by an agency, the agency shall immediately suspend use of all ALPRs and ALPR data until the State Attorney General has determined that the agency has taken sufficient action to remedy and prevent further such noncompliance.

(E) In addition to these audit results, the State Attorney General shall publish annually a public report stating:

(i) the total number of ALPR units being operated by government agencies within the state;
(ii) the total number of ALPR plate scans;
(iii) the total number of plate scans retained;
(iv) the total number of searches of historical data;
(v) the total number of hotlist alerts, broken down by the reason for the alert;
(vi) the total number of criminal investigations in which ALPRs or ALPR data were used;
(vii) any data breaches or unauthorized use of ALPRs or ALPR data;
(viii) a list of audits completed by the State Attorney General;
(ix) any other information deemed appropriate by the State Attorney General.

Editor's note. *Some states require the statewide collection and publication of aggregated data about ALPR use by policing agencies. E.g., Md. Pub. Safety Code § 3-509(e); 23 Vt. Stat. § 1607(e). These data facilitate appropriate oversight and may be valuable for future legislative and regulatory efforts.*

(F) The State Attorney General shall determine an appropriate minimum plate read accuracy rate for any ALPR used by an agency. Pending such determination, the minimum acceptable plate read accuracy rate shall be 85%.

IX. REMEDIES

(A) **Civil Cause of Action**: Any person or entity injured as a result of an agency's violation of this Act shall have a civil cause of action against such agency for damages (but not less than liquidated damages in the amount of $10,000) and reasonable costs and attorneys' fees. A court shall award punitive damages in an amount no less than $10,000 if the agency's violation of this Act was willful. The unauthorized use, retention, or sharing of data regarding an individual or entity's vehicle or license plate shall constitute a cognizable injury under this Act.

(B) **Injunctions**: The State Attorney General or any court of this State may prohibit an agency from using or acquiring any ALPRs, ALPR systems, or ALPR data where necessary to stop ongoing substantial violations or this Act, or to prevent future substantial violations of this Act.

(C) **Administrative Remedies**: Violation of this Act by an employee of a law enforcement agency shall be grounds for termination, demotion, or any other appropriate consequences for such employee.

(D) **Exclusion**: Neither ALPR data obtained in violation of the terms of this Act nor any evidence resulting therefrom shall be used against a criminal defendant in any state or local prosecution.

Editor's note. *California's ALPR statute creates a private right of action, authorizing courts to award liquidated and actual damages, and punitive damages in the case of willful or reckless disregard of the law. Cal. Civ. Code § 1798.90.54. Some ALPR statutes also include criminal penalties for violations. See, e.g., Ga. Code § 35-1-22(d)(1); Md. Pub. Safety Code § 3-509(b)(2); Utah. Code 1953 § 41-61-2006. The purpose of specifying that the unauthorized use, retention, or sharing of data constitutes a cognizable injury is to ensure that individuals subjected to unlawful ALPR surveillance have standing to sue under the Act. This provision may need to be modified in light of state standing requirements.*

X. PREEMPTION

Nothing in this Act shall be construed to preempt or supersede any other law or regulation imposing additional requirements on agencies related to the use of ALPRs or ALPR data, except to the extent that such law or regulation requires the retention of ALPR data by an agency for a period longer than that authorized by this Act.