State-Level Automatic License Plate Reader Privacy Guardrails Model Bill

Section 1. Definitions.

(A) "Automatic License Plate Reader (ALPR) system" shall mean a system, software, or computer algorithm, whether used independently or in combination with one or more mobile or fixed automated cameras, that is used to convert images of license plates into computer-readable data. An ALPR system shall not include cameras whose collection of images and other data is only activated when a vehicle within its field of view engages in a specific unlawful driving behavior, such as speeding or driving through a red light.

(B) "Captured plate data" shall mean the GPS coordinates, date and time, photograph, license plate number, and any other data captured by, derived, or inferred from any automatic license plate reader system, including but not limited to make, model, color, and other vehicle-related characteristics.

(C) "End-To-End Encryption" shall mean a security standard in which collected data is encrypted and stored on the system of the person or entity on whose behalf the data was collected and which can only be decrypted by a specific intended recipient, leaving the content unreadable to service providers, intermediaries, and any other unauthorized person or entity during its storage and transit.

(D) "Government entity" shall mean a department or agency of the state of [insert State name] or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(E) "Hot list" shall mean a database of compiled license plate and other vehicle identifying information that (1) is maintained in a manner that ensures it is and remains accurate, relevant, timely, and complete, and (2) reflects a law enforcement-related, government entity's determination that a vehicle or an individual associated with a vehicle is relevant and material to a specific ongoing criminal or missing persons enforcement effort or investigation.

(F) "Secured area" shall mean an area, enclosed by clear boundaries, to which access is limited and not open to the public and entry is only obtainable through specific access-control points.

Section 2. Restrictions on use.

(A) Except as provided for in Section 2(B), it shall be unlawful for any government entity to operate or use an automatic license plate reader system or the data therefrom.

(B) An automatic license plate reader system and the data therefrom may be operated or used by a government entity only:

(1) For the comparison of captured plate data with hot list data to determine if a vehicle scanned by an ALPR system is relevant and material to an investigation of a vehicle that is:

(a) Unregistered or uninsured;

(b) In violation of the inspection requirements set forth in section [insert citation to state vehicle inspection law];

(c) Registered to an individual for whom there is an outstanding felony warrant;

(d) Associated with a missing person;

(e) Stolen; or

(f) Related to or involved in a felony.

(2) By parking enforcement entities for regulating the use of parking facilities;

(3) For the purpose of controlling access to secured areas; or

(4) For the purpose of electronic toll collection.

(C) For the allowed uses under Section 2(B)(1)(a) and (b), it shall be unlawful to intentionally target enforcement towards a population based on race, ethnicity, or income level in a manner that exceeds that group's proportion of the overall population within the enforcing government entity's jurisdiction;

(D) It shall be unlawful to operate or utilize any ALPR system whose operation is not fully compliant with the provisions of this Act.

Section 3. Protections.

(A) Captured plate data collected by or on behalf of a government entity, as authorized pursuant to Section 2(B), shall not be used, shared, or accessed for any other purpose and shall be deleted after 48 hours, except that such data may be retained:

(1) For as long as such captured plate data is needed as evidence of specific unlawful conduct enumerated in Section 2(B)(1);

(2) For as long as such captured plate data is needed to support the assessment and collection of a toll pursuant to Section 2(B)(4);

(3) Pursuant to a Section 4(A) preservation request;

(4) Pursuant to a disclosure order sought pursuant to Section 4(B); or

(5) Pursuant to a valid, court issued, probable cause warrant or other valid court order.

(B) Notwithstanding the provisions of Section 3(A), captured plate data collected by or on behalf of a government entity, as authorized pursuant to Section 2(B), may only be used, shared, or accessed by an out-of-state person or entity pursuant to a valid, court issued, probable cause warrant or other valid court order.

(C) Any government entity that uses an automatic license plate reader system pursuant to Section 2(B)(1) must update those systems from the databases enumerated in Section 2(B)(1) in real-time, at the beginning of each shift, or whenever such updates are available.

(D) The security of all data collected by an automatic license plate readers system by or on behalf of a law enforcement agency shall be protected in storage and in transit using end-to-end encryption.

Section 4. Preservation and Access.

(A) Preservation request.

(1) A government entity that operates or uses an automatic license plate reader system, upon the written request of a government entity or a defendant in a criminal case, shall take all necessary steps to preserve specified captured plate data in its possession pending the issuance of a court order sought pursuant to Section 4(B), if:

(a) The requesting government entity or defendant in a criminal case requests such retention and specifies in a written, sworn statement:

(i) The particular camera or cameras for which captured plate data must be preserved or the particular license plate for which captured plate data must be preserved;

(ii) The date or dates and timeframes for which captured plate data must be preserved; and

(iii) That a court order for the retention and disclosure of captured plate data will be sought, pursuant to Section 4(B), in a court of competent jurisdiction within seven days of the transmission of the preservation request.

(B) A government entity or defendant in a criminal case may apply for a court order for the extended retention and disclosure of captured plate data, which shall be issued by any court of competent jurisdiction if the government entity or defendant in a criminal case offers specific and articulable facts showing there is probable cause to believe the captured plate data is relevant and material to an ongoing felony criminal or missing persons investigation, prosecution, or defense.

(C) Captured plate data retained by a government entity for more than 48 hours pursuant to a Section 4(A) preservation request shall be immediately destroyed if:

(1) An application for a court order, pursuant to Section 4(B), is not made within seven days of the preservation request, or

(2) The application for the court order, made pursuant to Section 4(B), is denied.

(D) Notice of a data deletion-triggering event, as enumerated in Section 4(C)(1) or (2), shall be provided within 24 hours of its occurrence by the person or entity who made the Section 4(A) preservation request to the recipient of that request.

(E) A government entity may purchase, obtain, receive, or use privately captured plate data only pursuant to a valid, court issued, probable cause warrant.

Section 5. Private ALPR Use-Related Limitations

(A) A government entity shall not request or demand a private operator or user of an ALPR system provide access to an ALPR camera, ALPR data, a searchable ALPR system, or the search results generated by an ALPR system unless the government entity has a judicially-issued, probable cause warrant for specific ALPR data which is related to a specific, ongoing criminal investigation for which ALPR use is authorized under this Act.

(B) A government entity may not accept access to private ALPR cameras, data, or systems, or the search results generated therefrom from a private person or entity, unless:

(1) The private person or entity was the party on whose behalf the ALPR data was collected;

(2) The private person or entity wishes to voluntarily provide the data for no monetary or other compensation;

(3) The private person or entity, in providing the data, asserts that the ALPR data may be relevant to the investigation of a specific crime; and

(4) The specific crime to which the ALPR data may be relevant was committed:

(a) On the private person's or entity's property;

(b) Against private person's or entity's customer; or

(c) Against the private person's or entity's employee.

(C) Any private person or entity who operates an ALPR camera or ALPR system in a place of public accommodation shall place an easily readable sign within 10 feet of each camera location notifying the public that an ALPR camera is

in use in the area and that it is scanning and capturing information about every vehicle within its viewing range.

Section 6. Data Sharing and ALPR access.

(A) Any government entity that uses automatic license plate reader systems pursuant to Section 2(B) shall:

(1) Not share or otherwise provide access to collected ALPR data unless the requesting party:

(a) Is a government entity that agrees not to further share the data unless otherwise required by law; and

(b) Has a judicially issued, probable cause warrant for the specific data.

(2) Not provide any other entity with direct access to the ALPR system.

(B) No government entity may receive ALPR data from a private entity, or access thereto, unless the specifically provided data is alleged to be relevant to the investigation of a specific crime committed on the private person's or entity's property or against a person who lives, works, or was an authorized visitor to the private person's or entity's property.

(C) No government entity may request ALPR data, or access thereto, from a private entity unless the government entity has a judicially authorized, probable cause warrant for the requested ALPR data.

Section 7. Reporting.

(D) Any government entity that uses automatic license plate reader systems pursuant to Section 2(B) shall:

(1) Consistent with the provisions of this Act, adopt a policy governing use of the system, prohibiting non-essential data collection and sharing, and protecting the security of data that is collected, the entirety of which shall be conspicuously posted on the government entity's Internet website;

(2) Report annually on its automatic license plate reader practices and usage to the state or local legislature that governs the government entity. The report must also be conspicuously posted on the government entity's Internet website. The report shall include:

(a) The number of license plates scanned;

(b) The names of the hot lists against which captured plate data were checked, and the number of matches generated by each hot list;

(c) The number of matches, by hot list, that resulted in arrest and prosecution;

(d) The number of preservation requests received under Section 4(A);

(e) The number of preservation requests issued under Section 4(A), broken down by the number of preservation requests issued to other government entities and the number of preservation requested issued to private automatic license plate reader systems;

(f) The number of disclosure orders received under Section 4(B);

(g) The number of times ALPR data was shared with or accessed by another government entity;

(h) The number of times ALPR data was shared or accessed pursuant to a judicial warrant; and

(i) Any changes in policy that affect privacy concerns.

Section 8. No captured plate data and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the State of [insert state name], or a political subdivision thereof, if the collection or disclosure of that information was or would be in violation of this Act, unless such evidence is exculpatory in a criminal trial or proceeding.

Section 9. Penalties.

(A) Any person who violates the provisions of this Act shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this Act has injured his business, his person, or his reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him on account of violation of the provisions of this Act, or liquidated damages of one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

Section 10. Privacy.

(A) Captured plate data shall not be considered a public record for the purposes of [insert citation to state open records law].

(B) Notwithstanding Section 10(A), the following information shall be considered a public record for the purposes of [insert citation to state open records law]:

(1) An ALPR system's audit, use, and access logs and data; however, in responding to a valid request, any individual license plate information or other vehicle-specific identifying information, such as vehicle photographs and information regarding a vehicle's make, model, or color, shall be redacted from the responsive documents and data; and

(2) Data and information regarding a vehicle personally owned or leased by the [name of open records law] requestor during the period of

ownership or lease; however, a request for such information shall only be permitted where, as part of the request:

(a) The requestor affirms, through a notarized, sworn statement, that the requester is the sole owner/lessor of the vehicle, and that no one other than the requestor drives the vehicle more than 10% of its total trips; or

(b) Where the requester is not the sole owner/lessor of the vehicle, or one or more other persons drives the vehicle more than 10% of its total trips, the primary requestor, through a notarized, sworn statement:

(i) Identifies every owner/lessor of the vehicle and every driver of the vehicle who drives the vehicle more than 10% of its trips;

(ii) Affirms that neither the primary requestor nor any other identified owner(s)/lessor(s) of the vehicle or other identified driver(s) is subject to an outstanding order of protection involving the primary requestor or any other identified owner(s), lessor(s), or identified driver(s) of the vehicle; and

(iii) Every owner, lessor, and driver identified pursuant to Section 10(B)(2)(b)(i) signs the request, thereby joining the primary requestor as a co-requestor in making the request.

(c) For purposes of Section 10(B)(2), the terms "requestor", "co-requestor", "owner", "lessor", and "driver" shall only refer to human persons, and not any business, corporate, or other non-human entities.

Section 11. Severability.

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. Effective Date.

This Act shall take effect upon passage.