House of Representatives

General Assembly

File No. 536

February Session, 2026

Substitute House Bill No. 5449

House of Representatives, April 9, 2026

The Committee on Judiciary reported through REP. STAFSTROM of the 129th Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

AN ACT CONCERNING AUTOMATED LICENSE PLATE READER SYSTEMS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective from passage*) (a) As used in this section and sections 2 and 3 of this act:

(1) "Automated license plate reader system" means a mobile or fixed electronic image recording device that is capable, in combination with computer programs or algorithms, of converting images of license plates or vehicle descriptors into computer-readable data;

(2) "Automated license plate reader data" includes any data captured, recorded, stored, processed or derived from an automated license plate reader system, including, but not limited to, license plate characters, vehicle still or video images, vehicle attributes, location data, time stamps and metadata;

(3) "Gender-affirming health care services" has the same meaning as provided in section 52-571m of the general statutes;

(4) "Hotlist" means a list of registration numbers displayed on license plates maintained for comparison against a registration number obtained by an automated license plate reader system;

(5) "Law enforcement agency" means a department or agency for which a law enforcement officer is an employee of or otherwise paid by or acting as an agent of, including, but not limited to, a municipal police department or the Division of State Police within the Department of Emergency Services and Public Protection;

(6) "Public agency" has the same meaning as provided in section 1-200 of the general statutes; and

(7) "Reproductive health care services" has the same meaning as provided in section 52-571m of the general statutes.

(b) (1) On and after October 1, 2026, no public agency or law enforcement agency may operate an automated license plate reader system or use automated license plate reader data, except as follows:

(A) A public agency may operate an automated license plate reader system or use automated license plate reader data for the following purposes: (i) Performing weigh station duties; (ii) monitoring or maintaining the agency's vehicles or equipment; (iii) assisting in the control of access to a secured area; (iv) conducting traffic analytics; or (v) enforcing traffic violations and collecting associated fines through the use of work zone speed control systems, as defined in section 13a-261 of the general statutes, and automated traffic enforcement safety devices, as defined in section 14-307b of the general statutes; and

(B) A law enforcement agency may operate an automated license plate reader system or use automated license plate reader data for the following purposes: (i) Comparing such data with (I) data contained in a hotlist, (II) records of the Connecticut Online Law Enforcement Communications Teleprocessing System, (III) data contained in the Federal Bureau of Investigations Kidnapping and Missing Persons list, (IV) data contained in the Connecticut Criminal Justice Information

System, (V) data contained in the Federal Terrorist Screening Database, (VI) data contained in the National Crime Information Center database, or (VII) data contained in the National Center for Missing and Exploited Children database; or (ii) entering a license plate number into an automated license plate reader system upon a law enforcement officer's determination that data in the system may (I) be relevant and material to a specific active investigation of a criminal offense in which there is reasonable suspicion that the offense has been or is being committed, provided any access by an officer of automated license plate reader data for such purpose shall result in a record of the factual basis for the access and any associated case number for the complaint or incident that is being investigated and is the basis for the access, (II) assist in the apprehension of an individual with an outstanding felony warrant, (III) assist in locating a missing or endangered individual, or (IV) assist in the recovery of a stolen motor vehicle.

(2) Any automated license plate reader data collected or held by a public agency or law enforcement agency shall not be retained for a period in excess of thirty days, or for a shorter period when required pursuant to the terms of a contract between a public agency or law enforcement agency with a private vendor that accesses an automated license plate reader system or stores such data, unless such data is being retained (A) pursuant to a warrant or court order issued by a judge or magistrate on behalf of the state or federal judicial branches, or pursuant to court rules governing the preservation of evidence, (B) for the purpose of collecting highway usage fees if such fees exist, provided such data is deleted not later than thirty days following the collection of such fees, or (C) as evidence in an active criminal investigation or prosecution, provided (i) at the time such data is designated for retention, such retention is approved by a supervisory law enforcement officer and documented by the law enforcement agency in a record stating the factual basis for such retention and any associated case number for the investigation or prosecution to which the data relates, and (ii) such data is deleted upon the conclusion of the investigation if no criminal charges are filed, or upon the final disposition of the criminal case to which the data relates, including the exhaustion of all

direct appeals, whichever occurs first, unless otherwise required to be retained under subparagraph (A) of this subdivision. Any other access to such data beyond an initial seven-day retention period, but prior to the end of such thirty-day retention period, shall be upon the issuance of a warrant by a judge or magistrate on behalf of the state or federal judicial branches.

(c) On and after October 1, 2026, no public agency or law enforcement agency operating an automated license plate reader system or using automated license plate reader data pursuant to subsection (b) of this section may:

(1) Use or assist in the use of automated license plate reader data to monitor or investigate an individual based on such individual's actual or perceived race, ethnicity, criminal history, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality or income level;

(2) Use or assist in the use of an automated license plate reader data system or automated license plate reader data for the purpose of identifying an individual engaged in an activity protected under the First Amendment to the United States Constitution;

(3) Use or assist in the use of an automated license plate reader data system or automated license plate reader data for the purpose of investigating a suspected immigration violation or otherwise assisting in any civil or criminal immigration enforcement activity;

(4) Use or assist in the use of an automated license plate reader data system or automated license plate reader data for the purpose of investigating or prosecuting any individual who has sought, received, or provided reproductive health care services or gender-affirming health care services;

(5) Unless authorized pursuant to section 29-6d of the general statutes, collect automated license plate reader data on the premises or within a distance established by the Police Officer Standards and

Training Council pursuant to section 2 of this act, of a reproductive or sexual health facility, as defined in section 42-515 of the general statutes, that primarily provides gender-affirming health care services or a nonprofit or community organization that primarily serves immigrant communities, excluding any property under federal jurisdiction, provided such facility or organization notified the Police Officer Standards and Training Council of such facility's or organization's location;

(6) Share or provide access to automated license plate reader data, unless the individual or entity requesting such data or access is (A) a public agency or law enforcement agency of this state, (B) a law enforcement agency of the state of New York or Rhode Island or the Commonwealth of Massachusetts or a municipality of said states or commonwealth or a multijurisdictional task force of which a public agency or law enforcement agency of this state is a participating member, provided (i) such requesting law enforcement agency or task force provides a written declaration affirming that any data received will be used in compliance with the prohibitions set forth in this section, and will not be used for an immigration investigation or enforcement action or to investigate or prosecute any individual who has sought, received or provided reproductive health care services or gender-affirming health care services and will not be further disclosed except as permitted by law, and (ii) in the case of a multijurisdictional task force, such specific data requested is approved by the head of such task force or such head's designee and is directly and reasonably relevant to a specific investigation of such task force, (C) any other law enforcement agency other than those of this state or described in subparagraph (B) of this subdivision, including any federal law enforcement agency, if such requesting law enforcement agency has a judicially issued probable cause warrant for the specific data requested, or is requesting specific data on an individual identified as a possible match in the Federal Terrorist Screening Database, or (D) is an individual requesting data regarding a motor vehicle registered in such individual's name, provided if a motor vehicle has more than one owner, lessor or regular user, all such owners, lessors and regular users join in the request and

are natural persons;

(7) Participate in a system or network that shares automated license plate reader data, or provide to, or access such data through any multistate, intrastate, or national data-sharing system or network unless such system or network requires, as a condition of participation in or access to such system or network, execution of a written declaration by each participant affirming that: (A) Any data obtained will be used solely in compliance with this section and other laws of this state; and (B) such participant will not share or use such data, except in compliance with the provisions of this section; and

(8) Permit a public agency to have real-time, bulk or automatic access to automated license plate reader data, unless such data is in response to a documented, case-specific request and the sharing of such data is not otherwise prohibited under this subsection.

(d) Automated license plate reader data shall not be disclosable under the Freedom of Information Act pursuant to chapter 14 of the general statutes. Any of the following information shall be disclosable pursuant to said act:

(1) Locations of any still or video image recording device used as part of an automated license plate reader system; and

(2) Any data, other than automated license plate reader data, derived from any audit of an automated license plate reader system, usage logs for such system and logs detailing access to automated license plate reader data, provided any such data disclosable under this subsection has all automated license plate reader data redacted from otherwise disclosable data.

(e) Not later than January 1, 2027, a public agency, other than a law enforcement agency, that operates an automated license plate reader system or uses automated license plate reader data shall adopt and publicize a written automated license plate reader system usage and privacy policy prior to using or acquiring an automated license plate

reader system or automated license plate reader data. Such policy shall comply with all applicable provisions of this section and include safeguards and standards substantially equivalent to those required under the model policy adopted under section 2 of this act.

(f) (1) On and after the effective date of this section, no public agency or law enforcement agency may enter into any contract or agreement with a private vendor that accesses an automated license plate reader system or stores, processes, transmits or accesses automated license plate reader data on behalf of the public agency or law enforcement agency, for the purpose of selling, sharing, transferring, disseminating or otherwise providing access to such data except as expressly authorized by this section.

(2) On and after the effective date of this section, any contract or agreement entered into between a public agency or law enforcement agency and a private vendor for the purpose of the provision of services associated with the use of an automated license plate reader system or use or storage of automated license plate reader data shall expressly require such vendor comply with the provisions of this section in the same manner as such provisions are applicable to the contracting public agency or law enforcement agency and shall expressly prohibit the vendor from retaining, using or disclosing automated license plate reader data for any purpose other than in fulfilling the vendor's contractual obligations.

(3) Any vendor that entered into a contract or an agreement pursuant to this subsection shall be considered an agent of the contracting public agency or law enforcement agency for purposes of services provided pursuant to the contract or agreement and shall be subject to the same provisions of this section as are applicable to such public agency or law enforcement agency.

(g) On and after October 1, 2026, a public agency or law enforcement agency may be subject to an action by any aggrieved individual for injunctive or declaratory relief, including a determination of past violations, if an officer, employee or other individual otherwise paid by

or acting as an agent of such agency violates any provision of subsection (b), (c) or (d) of this section. If the alleged violation that forms the basis of an action under this subsection is committed by any vendor contracting with a public agency or law enforcement agency, as described in subdivision (3) of subsection (f) of this section, the vendor shall be liable for such violation, not the law enforcement agency or public agency. Such action may be brought in the superior court for the judicial district in which the aggrieved individual resides. If an aggrieved individual prevails and an order of injunctive relief is issued, such aggrieved individual may be entitled to recover court costs and reasonable attorney's fees associated only with an action or that portion of an action concerning a request and order for injunctive relief. An action under this subsection shall be privileged with respect to assignment for trial.

Sec. 2. (NEW) (*Effective from passage*) (a) Not later than December 1, 2026, the Police Officer Standards and Training Council shall adopt a model policy governing law enforcement agency acquisition and use of automated license plate reader systems and automated license plate reader data. Such policy shall direct agencies to act in accordance with section 1 of this act, including permissible and prohibited uses of such system and any automated license plate reader data, whether derived from such system or acquired in any other manner. In addition to detailing such permissible and prohibited uses of such system or data, such policy shall, at a minimum: (1) Develop standards for the use of a hotlist, including the sources from which a hotlist may be compiled, supervisory approval requirements for use and management of, access to and validation procedures for the data on any hotlist, including time limitations for the inclusion of such data on a hotlist, (2) provide for data retention limits in accordance with subdivision (2) of subsection (b) of section 1 of this act, (3) establish data access and sharing requirements in accordance with subsection (c) of section 1 of this act, including internal access controls and supervisory review and conditions under which such data may be shared with other public agencies or law enforcement agencies, (4) provide for a supervisory responsibility and accountability structure, including designation of an officer or unit

responsible for oversight of automated license plate reader system use and compliance with any policy adopted in accordance with the provisions of this section, (5) establish training requirements, including initial and periodic training for any officer or employee authorized to access the system or data, (6) establish audit and logging requirements, including the creation and retention of access logs sufficient to ensure compliance and facilitate independent review, of which the logs shall include documentation of access to and retention of automated license plate reader data pursuant to subdivision (2) of subsection (b) of section 1 of this act, including, but not limited to, (A) the number of times such data is retained, and (B) the duration of such retention, and require that such audits be conducted not less than quarterly, (7) establish public transparency standards and requirements, including publication of agency-specific usage policies for an automated license plate reader system and annual statistical reports detailing such usage, (8) establish the distance described in subdivision (5) of subsection (c) of section 1 of this act, and (9) contain provisions concerning compliance with subsection (f) of section 1 of this act concerning contracting with vendors for services associated with access to an automated license plate reader system or storage of, processing of, transmission of or access to automated license plate reader data.

(b) Not later than January 1, 2027, each law enforcement agency shall adopt and implement the policy developed pursuant to subsection (a) of this section, or a policy that provides greater privacy protections than that which are in the policy developed pursuant to said subsection (a). Such policy shall be in effect until regulations are adopted pursuant to this section, at which point such policy shall be supplanted by any such regulation.

(c) (1) Not later than January 1, 2028, the Commissioner of Emergency Services and Public Protection shall, in consultation with the Police Officer Standards and Training Council, adopt regulations, in accordance with the provisions of chapter 54 of the general statutes, to enact a policy that at a minimum, satisfies the provisions of subdivisions (1) to (9), inclusive, of subsection (a) of this section and section 1 of this

act.

(2) Not later than January 1, 2033, and at least once during each five-year period thereafter, the commissioner shall, in consultation with the Police Officer Standards and Training Council, adopt regulations in accordance with the provisions of chapter 54 of the general statutes. Such regulations shall (A) comply with the provisions of this section and section 1 of this act and shall not reduce or limit the protections afforded by said sections or any minimum standards established by said sections, and (B) be based on a consideration of any changes in law, technology and best practices since the previous adoption of regulations pursuant to this section.

(3) Any regulation adopted pursuant to this section shall be binding upon all law enforcement agencies.

Sec. 3. (NEW) (*Effective from passage*) (a) The Police Officer Standards and Training Council, in consultation with the Commissioner of Emergency Services and Public Protection and the Institute for Municipal and Regional Policy at The University of Connecticut, shall develop and promulgate a standardized form for reporting automated license plate reader system usage, including, but not limited to, (1) the number of (A) license plates scanned, (B) searches performed by the law enforcement agency as a result of automated license plate reader system use and the reason for any such search, (C) times automated license plate reader data was shared with or accessed by another entity, the identity of each of those entities and the reason for sharing the data, (D) times automated license plate reader data was shared or accessed pursuant to a judicial warrant, and (E) instances, if any, when data was retained longer than permissible pursuant to subdivision (2) of subsection (b) of section 1 of this act, and (2) any changes to the law enforcement agency's data collection, retention or sharing policies that affect privacy of automated license plate reader data.

(b) Each law enforcement agency shall, not later than January thirty-first following a calendar year during which the law enforcement agency used an automated license plate reader system pursuant to

subsection (b) of section 1 of this act, submit a report detailing such usage to the Institute for Municipal and Regional Policy at The University of Connecticut using the standardized form promulgated pursuant to subsection (a) of this section and publish such report on the law enforcement agency's Internet web site.

(c) Not later than January thirty-first of each year, any public agency, other than a law enforcement agency, that uses an automated license plate reader system pursuant to subsection (b) of section 1 of this act, shall publish on the agency's Internet web site an annual report containing the information described in subsection (a) of this section as it pertains to such agency for the previous calendar year.

(d) Not later than July 30, 2027, and annually thereafter, the Institute for Municipal and Regional Policy at The University of Connecticut shall compile, analyze and summarize the reports submitted pursuant to subparagraph (a) of this subsection and shall submit, in accordance with section 11-4a of the general statutes, a consolidated report regarding automated license plate reader system usage and any recommendations for legislation to the Governor and the joint standing committees of the General Assembly having cognizance of matters relating to public safety and the judiciary.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*from passage*	New section
Sec. 2	*from passage*	New section
Sec. 3	*from passage*	New section

Statement of Legislative Commissioners:
In Section 3(a)(1)(B), "searches performed by the law enforcement agency" was changed to "searches performed by the law enforcement agency as a result of automated license plate reader system use" for clarity.

JUD *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

The bill makes various changes related to the use of automated license plate reader (ALPR) systems by law enforcement and other public agencies and does not result in a fiscal impact, as described below.

Section 1 allows certain individuals to bring an action in Superior Court for alleged violations of the bill's provisions, resulting in no fiscal impact to the state. The court system disposes of over 250,000 cases annually and the number of cases is not anticipated to be great enough to need additional resources.

Section 2 requires the Police Officer Standards and Training Council (POSTC) to adopt a model policy governing law enforcement acquisition and use of ALPR data and does not result in a fiscal impact because POSTC has already adopted an ALPR model policy. To the extent that revisions to the current policy are needed to meet the requirements of the bill, POSTC can accomplish this within existing resources.

Section 2 also requires the Department of Emergency Services and Public Protection (DESPP) to adopt related regulations, which the agency has existing expertise to do.

Section 3 sets various ALPR reporting requirements and does not

have a fiscal impact because it is expected that agencies can comply within existing resources.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis

sHB 5449

AN ACT CONCERNING AUTOMATED LICENSE PLATE READER SYSTEMS.

SUMMARY

Starting October 1, 2026, this bill restricts law enforcement agencies and other public agencies from using automated license plate reader (ALPR) systems or ALPR data, except for certain listed reasons. Among other things, it:

1. sets a 30-day limit on how long agencies can keep this data unless certain conditions are met (such as its use in an active criminal investigation), and in some cases requires agencies to get a warrant if they seek to access the data more than seven days after they obtained it;

2. specifically prohibits several uses of ALPR systems or data, such as for investigating suspected immigration violations;

3. establishes requirements and restrictions for ALPR contracts between agencies and private vendors;

4. allows individuals aggrieved by violations to seek injunctive or declaratory relief;

5. requires the Police Officer Standards and Training Council (POST) to adopt a model ALPR usage policy and the Department of Emergency Services and Public Protection (DESPP) to adopt related regulations for implementation by law enforcement agencies;

6. requires POST, in consultation with UConn's Institute for Municipal and Regional Policy (IMRP), to develop a

standardized form for reporting ALPR system usage; and

7. sets related reporting requirements for law enforcement agencies, other public agencies, and UConn's IMRP.

Under the bill, an "ALPR system" is a mobile or fixed electronic image recording device that, in combination with computer programs or algorithms, can convert images of license plates or vehicle descriptors into computer-readable data.

"ALPR data" is any data that an ALPR system captures, records, stores, or processes, or that is derived from the system. This includes license plate characters, vehicles' still or video images, vehicle attributes, location data, time stamps, and metadata.

EFFECTIVE DATE: Upon passage

§ 1 — ALPR USAGE AND PROHIBITIONS

Permissible Uses

Starting on October 1, 2026, the bill prohibits law enforcement agencies (such as municipal police departments or the State Police) and public agencies (see BACKGROUND) from operating ALPR systems or using ALPR data, except under the following conditions.

Public Agency Uses. Under the bill, public agencies may operate these systems or use this data to:

1. perform weigh station duties;

2. monitor or maintain their own vehicles or equipment;

3. help in controlling access to secured areas;

4. analyze traffic; or

5. enforce traffic violations and collect associated fines by using work zone speed camera systems and automated traffic enforcement safety devices ("red light cameras").

Law Enforcement Uses. The bill allows law enforcement agencies to operate these systems or use this data to compare with data in:

1. a hotlist (a list of registration numbers displayed on license plates, kept for purposes of this comparison);
2. the Connecticut Online Law Enforcement Communications Teleprocessing (COLLECT) system;
3. the FBI's Kidnapping and Missing Persons list;
4. the Connecticut Criminal Justice Information System;
5. the federal Terrorist Screening Database;
6. the National Crime Information Center (NCIC) database; or
7. the National Center for Missing and Exploited Children database.

The bill also allows law enforcement agencies to enter license plate numbers into an ALPR system if an officer determined that system data may:

1. help to apprehend someone with an outstanding felony warrant,
2. help to locate a missing or endangered person or to recover a stolen vehicle, or
3. be relevant and material to a specific active criminal investigation.

For criminal investigations, this use is allowed only if there is a reasonable suspicion that the offense has been or is being committed. The agency must keep a record of (1) the factual basis for accessing the data and (2) any associated case number for the complaint or incident.

Retention Limit. The bill generally allows public agencies or law enforcement agencies to keep ALPR data for only 30 days. But they must keep it for a shorter period if that is required by a contract between the

agency and a private vendor that accesses the system or stores the data.

These periods do not apply to data being kept:

1. under a state or federal judicial warrant or court order;

2. under court rules on preserving evidence;

3. for collecting highway usage fees (if they exist), but the data must be deleted within 30 days after the fee is collected; or

4. as evidence in an active criminal investigation or prosecution.

For this last reason, a supervisory law enforcement officer must approve the longer retention period, and the agency must keep a record of (1) the factual basis for keeping the data and (2) any associated case number. Unless a warrant, court order, or rules of evidence require otherwise, the data must be deleted upon the earlier of the (1) investigation's conclusion, if no charges are filed, or (2) case's final disposition, including all direct appeals being exhausted.

Under the bill, any other access to the data after the first seven days, and before the end of the 30-day retention period, is allowed only upon a state or federal judicial warrant or court order.

Specifically Prohibited Uses

The bill prohibits public agencies and law enforcement agencies from operating an ALPR system or using ALPR data for various purposes. These prohibitions apply starting on October 1, 2026.

Various Prohibitions. Specifically, it bars them from using or helping in the use of ALPR data to monitor or investigate someone based on their actual or perceived race, ethnicity, criminal history, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality, or income.

It also bars them from using or helping in the use of an ALPR system or ALPR data to:

1. identify someone engaged in an activity protected by the First Amendment;

2. investigate a suspected immigration violation or otherwise help in civil or criminal immigration enforcement; or

3. investigate or prosecute someone who has sought, received, or provided reproductive or gender-affirming health care services.

Collection Near Gender-Affirming Care Facilities or Facilities Serving Immigrants. The bill also generally bars public agencies and law enforcement agencies from collecting ALPR data at or near a (1) reproductive or sexual health facility that primarily provides gender-affirming health care services or (2) nonprofit or community organization that primarily serves immigrant communities. It requires POST to establish a distance for this prohibition (see below).

For these prohibitions to apply, the facility or organization must notify POST of its location. The prohibitions do not apply (1) if collecting the data would be allowed under the law on police body and dashboard cameras or (2) at properties under federal jurisdiction.

Information Sharing. The bill also restricts when these agencies can share or provide access to ALPR data. It allows them to do so only if the requesting person or entity is:

1. an individual requesting data for a vehicle registered in his or her own name (if a vehicle has multiple owners, lessors, or regular users, they all must be individuals and must join in the request);

2. another Connecticut public agency or law enforcement agency; or

3. under certain conditions, a law enforcement agency from another jurisdiction or multi-jurisdictional task force.

Under the bill, public agencies or law enforcement agencies can share ALPR data with a state or municipal law enforcement agency from

Massachusetts, New York, or Rhode Island, or a multi-jurisdictional task force of which the Connecticut agency is a member, but only if the requesting agency or task force affirms in writing that in using the data, it will comply with the bill's prohibitions and will not:

1. use it for immigration investigations or enforcement,

2. use it for investigations or prosecutions relating to reproductive or gender-affirming health care services, or

3. further disclose it except as allowed by law.

Additionally, for a task force, the group's head or designee must have approved the specific data request, and the data must be directly and reasonably relevant to a specific investigation.

The bill also allows Connecticut agencies or law enforcement agencies to share data with other law enforcement agencies (including federal ones), but only if the requesting agency has a judicially issued probable cause warrant for the specific data requested or is requesting specific data on a possible match in the federal Terrorist Screening Database.

Network Participation. Unless certain conditions are met, the bill bars public agencies and law enforcement agencies from (1) participating in a system or network that shares ALPR data or (2) giving data to or accessing it through a multi-state, intrastate, or national data-sharing system or network. This is allowed only if the system or network requires participants to execute a written declaration affirming that the data will be used solely in line with the bill and other Connecticut law and that they will not share or use the data except in line with the bill.

Bulk or Automatic Access. The bill also bars these agencies from allowing a public agency to have real-time, bulk, or automatic access to ALPR data, unless (1) in response to a documented, case-specific request and (2) the bill does not otherwise prohibit the data sharing.

Limits on Data Disclosure Under FOIA

The bill prohibits ALPR data from being disclosed under the Freedom of Information Act (FOIA). But it makes the following disclosable under FOIA:

1. the locations of ALPR recording devices (of video or still images) and

2. data other than ALPR data derived from a system audit, system usage logs, and data access logs, as long as ALPR data is redacted.

Required Policies for Public Agencies

The bill requires public agencies (other than law enforcement agencies) that operate ALPR systems or use ALPR data to adopt and make public a written usage and privacy policy. They must do this by January 1, 2027, and before they use or acquire a system or data. The policy must (1) comply with the bill's applicable provisions and (2) include standards and safeguards substantially equivalent to those required under POST's model policy (see below).

Contracts With Private Vendors

The bill sets restrictions on public agency or law enforcement agency contracts or agreements with private vendors that access ALPR systems, or store, process, transmit, or access this data, on the agency's behalf for various purposes (such as selling or sharing the data).

The contract must expressly require the vendor to comply with the bill's provisions in the same way as the bill applies to the agency, as applicable. It must expressly prohibit the vendor from keeping, using, or disclosing ALPR data for any purpose other than fulfilling its contractual obligations. The vendor is considered to be the agency's agent for the contractual services and is subject to the bill's provisions that apply to the agency.

These provisions do not apply to contracts that pre-dated the bill's passage.

Private Enforcement

Staring October 1, 2026, the bill allows an aggrieved individual to bring an action against a public agency or law enforcement agency for injunctive or declaratory relief, including a determination of past violations. This applies if the agency's officer, employee, or agent violates any of the bill's provisions on permissible or prohibited uses or data sharing (including under FOIA). If a vendor committed the violation, the vendor itself (and not the agency) is liable.

Under the bill, an aggrieved individual can bring the case in the judicial district where he or she lives. If the individual prevails and is granted an order for injunctive relief, the individual may be entitled to recover court costs and reasonable attorney's fees (but only with respect to the case, or part of it, related to seeking and getting the injunction).

These cases must be privileged (prioritized) with respect to trial assignment.

§ 2 — POST POLICY, LAW ENFORCEMENT ADOPTION, AND DESPP REGULATIONS

By December 1, 2026, the bill requires POST to adopt a model policy on law enforcement agencies' acquisition and use of ALPR systems and data. The policy must direct these agencies to comply with the bill, including allowed and prohibited uses of ALPR systems and data (however they acquired the data). The policy must also:

1. set standards for using a hotlist (including permissible sources) and supervisory approval requirements for using, managing, accessing, and validating hotlist data (including time limits to include data on a hotlist);

2. set data retention limits in line with the bill's requirements (see above);

3. set data access and sharing requirements in line with the bill, including internal access controls and supervisory review and conditions under which the data may be shared with other

agencies;

4. provide for a supervisory responsibility and accountability structure, including designating an officer or unit responsible for overseeing ALPR system use and complying with the policy;

5. set training requirements, including for officers and employees authorized to access the system or data;

6. set audit and logging requirements, including for access logs (see below), with audits done at least quarterly;

7. set public transparency standards and requirements, including for publication of agency-specific ALPR system usage policies and annual statistical reports on this usage;

8. set the distance for the general prohibition on collecting ALPR data near (a) facilities that primarily provide gender-affirming health care or (b) nonprofits or organizations that primarily serve immigrant communities (see above); and

9. include provisions on compliance with the bill's vendor-related provisions (see above).

The model policy's provisions on access logs must ensure compliance and facilitate independent review. The logs must document the access and retention of ALPR data, including how often the data is kept and for how long.

Law Enforcement Agency Adoption or Alternate Policy

The bill requires each law enforcement agency, by January 1, 2027, to adopt and implement either POST's model policy or another policy that gives greater privacy protections than the model policy. Law enforcement agency policies are in effect until DESPP's regulations are adopted (see below). Once adopted, the regulations supersede agency policies.

DESPP Regulations

By January 1, 2028, the bill requires the DESPP commissioner, in consultation with POST, to adopt regulations setting a policy in line with the requirements for POST's model policy and the bill's other provisions. By January 1, 2033, and at least every five years after, the commissioner, in consultation with POST, must update the regulations based on any changes in law, technology, or best practices. The updated regulations must not reduce or limit the bill's protections or minimum standards.

These regulations are binding on all law enforcement agencies.

§ 3 — STANDARD FORM AND REPORTING

Standardized Form

The bill requires POST, in consultation with DESPP and UConn's Institute for Municipal and Regional Policy (IMRP), to develop a standardized form for reporting ALPR system usage. The form must include the number of:

1. license plates scanned;
2. searches done by the law enforcement agency due to ALPR system use and the reasons why;
3. times ALPR data was shared with or accessed by other entities, their identities, and the reasons why;
4. times ALPR data was shared or accessed under a judicial warrant; and
5. any instances when the data was kept longer than allowed under the bill.

The form also must include any changes to the law enforcement agency's data collection, retention, or sharing policies that affect ALPR data privacy.

ALPR Usage Reporting

Under the bill, if a law enforcement agency uses an ALPR system, it must annually report to UConn's IMRP, using the standard form, and publish the report on the agency's website. If another public agency uses an ALPR system, it must post an annual report on its website about that usage, with the applicable information from the standard reporting form.

In either case, the reporting or posting is due by January 31 following any year when the agency uses an ALPR system.

IMRP Reporting

The bill requires UConn's IMRP to annually compile, analyze, and summarize the submitted reports and prepare a consolidated report on ALPR usage along with any legislative recommendations. The report must be sent to the governor and the Judiciary and Public Safety and Security committees, with the first report due by July 30, 2027.

BACKGROUND

Public Agencies

Under FOIA and the bill, a public agency generally includes any:

1. executive, administrative, or legislative office of the state or any political subdivision of the state and any state or town agency;

2. department, board, commission, authority, or official of the state or of any municipality, school district, or other district or other political subdivision;

3. committee of, or created by, any of these offices or officials;

4. judicial office, official, or body or committee, but only for administrative functions; and

5. person to the extent they are the functional equivalent of a public agency (CGS § 1-200(1)).

Related Bills

sSB 4, § 18 (File 285), favorably reported by the General Law Committee, prohibits the departments of transportation and motor vehicles, or law enforcement agencies, from entering or renewing contracts with ALPR users unless the contract bars the user from taking various actions.

sHB 5552, favorably reported by the Government Administration and Elections Committee, prohibits public agencies from entering into or renewing contracts with ALPR vendors unless the contract bars the vendor from taking various actions.

COMMITTEE ACTION

Judiciary Committee

Joint Favorable Substitute
Yea 32 Nay 9 (03/23/2026)