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)