

Automated License Plate Reader System Data Privacy Requirements and Breach Notification Laws

By: Duke Chen, Principal Analyst
August 12, 2026 | 2026-R-0125

Issue

Briefly describe (1) how the new law restricting law enforcement and other public agency use of automated license plate reader (ALPR) systems addresses certain data privacy concerns and (2) the existing data breach and notification laws.

Summary

This year, the Connecticut legislature passed a law setting various conditions and restrictions on the use of ALPR systems or associated data ([PA 26-14](#), §§ 13-15, as amended by [PA 26-76](#), § 46). Starting October 1, 2026, the act restricts law enforcement agencies (such as municipal police departments or the State Police), other public agencies, and private vendors under contract with them from using ALPR systems or ALPR data, except for specified reasons. Among other things, it:

1. sets a 21-day limit on how long agencies can keep this data unless certain conditions are met (such as its use in an active criminal investigation);
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; and
4. allows the attorney general or private parties to go to court to enforce specified violations and the Police Officer Standards and Training Council (POST) to take disciplinary action against law enforcement officers for certain malicious conduct.

These provisions are summarized in more detail below.

Separately, Connecticut law generally requires anyone in the state who owns, licenses, or maintains computerized data that includes personal information to notify affected Connecticut residents and the attorney general about a data security breach of certain personal information, or when it is reasonably believed to have been breached, without unreasonable delay within 60 days after discovering it. In these cases, the person who owns or licenses the data must also offer at least two years of free identity theft prevention and mitigation services if a resident's Social Security or Taxpayer Identification number is compromised. Failure to meet these requirements is an unfair trade practice and subject to enforcement by the attorney general ([CGS § 36a-701b](#)). More information is available on the attorney general office's [website](#).

Following a data breach, consumers may check or place a security freeze on their credit report. State law prohibits credit rating agencies from (1) charging a fee to place, remove, or temporarily lift a security freeze and (2) requiring a consumer, as a condition of placing a freeze, to limit claims he or she may have against the agency ([CGS §§ 36a-701](#) and [-701a](#)).

Several other laws require certain agencies, entities, or individuals to limit or restrict access to information they hold with varying degrees of specific technological considerations (for example, state contractors ([CGS §§ 4e-70](#)), and board of education contractors ([10-234aa](#) to [-234ff](#))). Also, a 2026 law requires Department of Banking licensees and Connecticut banks and credit unions to notify the department within three business days after a data security incident ([PA 26-51](#), § 1).

2026 ALPR Legislation

ALPR Definitions

Under the act, 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. But it does not include an image recording device that provides evidence used to enforce an offense specified in a state statute or municipal ordinance, including an automated traffic enforcement safety device (speed or red light camera), or those used as part of a work zone speed control system or a municipal school bus violation enforcement system.

“ALPR data” is any data that an ALPR system captures, records, holds or 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.

Permissible Uses

Starting October 1, 2026, the act prohibits public agencies, or private vendors under contract with them, from operating ALPR systems or using ALPR data, except under certain conditions.

Under the Freedom of Information Act (FOIA) and the act, 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\(1\)](#)).

Public Agency or Vendor Uses. Under the act, public agencies or private vendors under contract with them 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 control access to secured areas;
4. analyze traffic;
5. enforce parking regulations and collect associated fines, including (a) by a municipal parking authority or (b) on the grounds of a facility owned or operated by any other public agency and any garages or parking lots the facilities use (next to the facility or otherwise);
6. enforce motor vehicle property tax compliance; and
7. monitor and secure state facilities.

For these purposes, a “state facility” is any building (or part of one) owned, leased, occupied, controlled by, or used for business by an office or agency of the state executive, legislative, or judicial branch. This includes entities providing direct services on their behalf, but not state-owned property leased to a federal entity. It also includes these facilities’ grounds and any garages or parking lots the facilities use (next to the facility or otherwise).

Law Enforcement or Vendor Uses. The act allows law enforcement agencies or private vendors under contract with them to operate ALPR systems or use ALPR data to compare with data in:

1. a hotlist (a list of registration numbers on license plates, kept for this comparison) or internal hotlist addendum (see below);
2. the Connecticut On-Line 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 database; or
7. the National Center for Missing and Exploited Children database.

Under the act, an "internal hotlist addendum" is a hotlist that (1) is kept for use only at a specific state facility or facilities for which the list was made and by the public agency that made it and (2) may contain registration numbers shown on a vehicle license plate registered to a person identified as a potential threat to someone in the facility, the facility itself, or the agency operating it. A potential threat may be shown by a previous conviction for an offense involving threats of violence or harassment, or documented conduct involving threatened or attempted violence, harassment, or incitement to violence, against someone in the facility, the facility, or the agency. But an addendum item cannot be based on an arrest for, or conduct that is, solely constitutionally protected speech, conduct, or association (under the state or federal constitution).

The act also allows law enforcement agencies and their private vendors to enter license plate numbers into an ALPR system if an officer determined that system data may:

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

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

Retention Duration Limit. The act generally limits how long public agencies or private vendors under contract with them may keep ALPR data (regardless of how it was acquired) to only 21 days. But a shorter period applies if the contract between the agency and a private vendor that accesses the system or holds or stores the data requires it.

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 use fees (if they exist), but it must be deleted within 30 days after the fee is collected;
4. for analyzing traffic, if it is held, stored, or managed as de-identified, aggregated, or summarized data; or
5. 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 the purpose for keeping the data and any associated case number. Unless a warrant, court order, or evidence rules require otherwise, the data must be deleted upon (1) the investigation's conclusion, if no charges are filed; (2) if there is a conviction without a prison sentence, the case's final disposition, including exhaustion of all direct appeals; or (3) if there is a conviction with a prison sentence, the release of the last person imprisoned for a conviction to which the data relates.

The act also allows public agencies or their private vendors to keep ALPR data for more than 21 days if it may be needed to establish that a potential future offense, motor vehicle violation, or infraction (under an ordinance, statute, or regulation) is a subsequent one with a higher penalty than the previous one.

Additionally, if ALPR data is collected to enforce motor vehicle property tax compliance, it may be kept for longer than 21 days if the data is (1) kept expressly for that purpose; (2) not shared with anyone other than the municipality's tax assessor or the vehicle's registered owner; and (3) deleted after 90 days or following the tax assessor's determination of compliance, whichever occurs first.

Use as Evidence. Under the act, ALPR data is admissible as evidence in Connecticut courts, as long as it was collected or otherwise acquired, held, or stored in line with the act or obtained under a warrant issued by a Superior Court judge.

Specifically Prohibited Uses and Exceptions

The act prohibits public agencies from operating an ALPR system or using ALPR data for various purposes, starting October 1, 2026.

Various Prohibitions. Specifically, the act 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, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality, or income, or their perceived criminal history (except during an investigation of a potential crime for which an element of the offense is a prior conviction).

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

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

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

investigate or prosecute someone who sought, received, or provided reproductive or gender-affirming health care services that are legal under state law.

Collection Near Gender-Affirming Care Facilities or Facilities Serving

Immigrants. The act also generally bars the agencies from collecting ALPR data from a fixed ALPR system at or near a (1) reproductive or sexual health facility that primarily provides gender-affirming health care services that are legal under state law or (2) nonprofit or community organization that primarily serves immigrant communities.

Under the act, POST must establish the distance for these prohibitions (see its model policy below), and the facility or organization must notify POST about its location for the prohibitions to apply. The prohibitions do not apply (1) if collecting the data is allowed under the law on police body and dashboard cameras or (2) to properties under federal jurisdiction.

Information Sharing. The act 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 join in the request);
2. another Connecticut public agency; or
3. under certain conditions, a law enforcement agency from another jurisdiction or multi-jurisdictional task force.

Under the act, public 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 a 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 act'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 that are legal under Connecticut law, or
3. further disclose it except as Connecticut law allows.

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 act also allows Connecticut agencies to share data with other law enforcement agencies (including federal ones), but only if the requesting agency (1) has a judicially issued probable cause warrant for the requested data or (2) seeks specific data on a possible match in the federal Terrorist Screening Database.

Under the act, a Connecticut law enforcement agency must notify POST if, after sharing ALPR data with another state's or a federal law enforcement agency, it suspects that the other agency may have used the data in a way the act prohibits. POST must determine whether this occurred and, if so, direct each Connecticut law enforcement agency to stop sharing ALPR data with, or giving ALPR data access to, that agency.

Network Participation. Unless certain conditions are met, the act bars public 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 shared, accessed, or otherwise acquired data will be used solely in line with the act and other Connecticut law and that they will not share or use the data except as the act allows.

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

Limits on Data Disclosure Under FOIA and Exceptions

The act makes ALPR data confidential and prohibits it from being deemed a public record under FOIA. But it deems the following as public records, making them generally disclosable under FOIA:

1. locations of ALPR recording devices (of video or still images), unless the U.S. Department of Homeland Security funded the device's purchase (in whole or part) and the funding was conditioned on the device's location being confidential; and
2. data derived from an ALPR system audit, system usage logs, and data access logs, as long as ALPR data is redacted.

The act allows people to get, from the contracting public agency, ALPR data about vehicles registered in their name. But if a vehicle is also registered in someone else's name, that person also must consent to the disclosure.

Contracts With Private Vendors; Attorney General Enforcement

The act prohibits public agencies from entering or renewing contracts with private vendors related to ALPR system usage or data unless the contract bars the vendor from engaging in certain activities involving ALPR data collected in the state. This applies despite any contrary terms of service (such as conditions of use or vendor policies) that are incorporated by reference or other means.

Specifically, the contract must bar the vendor from:

1. selling the ALPR data;
2. sharing or transferring it with or to a third party without the contracting agency's express prior written authorization to do so for a specific purpose;
3. allowing anyone other than the contracting agency to access the ALPR data, unless the vendor must allow it due to a Connecticut or federal warrant or court order (but not a subpoena or demand of a grand jury investigation); or
4. holding or storing the contracting agency's ALPR data (a) with ALPR data it holds or stores under a contract with a different agency or other person or (b) in a way that does not align with industry-recognized data security practices, such as using encryption when sending or storing it. ([PA 26-76](#), § 46, removes the provision barring vendors from holding or storing the agency's ALPR data with ALPR data it has under a different contract.)

The contract also must bar the vendor from sharing or transferring ALPR data, or allowing access to it, if the vendor reasonably believes that it will be used to:

1. investigate a suspected immigration violation or otherwise help in immigration enforcement;
2. investigate or prosecute anyone for allegedly (a) seeking, providing, or receiving reproductive or gender-affirming health care services that are legal under Connecticut law or (b) helping someone else to do so (for example, by giving information, transportation, lodging, or material support for these activities); or
3. identify or impose civil or criminal liability on someone solely for an activity the state or federal constitution protects, including someone exercising the right to free speech, peaceable assembly, or petition the government for a redress of grievances, except as otherwise provided by state or federal law.

The act also prohibits public agencies from entering or renewing ALPR-related contracts with private vendors unless the contract requires (1) the vendor to consent to personal jurisdiction in Connecticut for legal proceedings and (2) Connecticut law to govern the contract.

Under the act, if a private vendor under contract with a public agency engages in any of the above prohibited conduct involving ALPR data collected in the state, the attorney general may bring an action against the vendor. In these cases, the court may grant appropriate relief, including injunctive or declaratory relief, damages, and any other relief the law allows. If the attorney general prevails, the court must order that any awarded damages are given to the injured person. The court may also award civil penalties against each defendant, up to \$2,500 per violation, to be deposited in the General Fund.

Private Enforcement

Starting October 1, 2026, the act allows an aggrieved individual to bring an action against a public 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 act's provisions on permissible or prohibited uses or data sharing (including under FOIA). If a private vendor committed the violation, or it engaged in any of the conduct prohibited under these contracts (see above) for ALPR data collected in the state, the vendor itself (and not the agency) is liable.

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

These cases must be privileged (prioritized) for trial assignment.

POST Disciplinary Action

Under the act, if a law enforcement officer is found to have knowingly accessed, used, or disseminated ALPR data with malicious intent for purposes beyond the act's allowable uses, the officer is subject to disciplinary action, such as suspension, cancellation, or revocation of his or her POST certification.

Other Provisions

The act also includes ALPR-related requirements regarding (1) policies for non-police public agencies, (2) a POST model policy and law enforcement adoption, (3) Department of Emergency Services and Public Protection regulations, and (4) ALPR system usage reporting.

For a full overview of the act, see OLR's Public Act Summary (forthcoming).

DC:ms