

PUBLIC SAFETY AND PRIVACY CONSIDERATIONS OF AUTOMATIC LICENSE PLATE READERS

Automatic license plate readers (ALPRs), sometimes called automated license plate recognition systems, are becoming an increasingly common law-enforcement technology in Illinois and across the United States. The systems use cameras and computer software to identify license plates and typically record the plate number, photograph of the vehicle, date, time and location of each detection. Modern systems can search millions of these observations rapidly and compare plates against databases of stolen vehicles, wanted persons, missing persons and vehicles associated with criminal investigations.

ALPRs can provide significant public-safety benefits. Police departments use them to identify stolen vehicles, locate missing or endangered persons, investigate shootings and other serious crimes, and reconstruct the movements of vehicles associated with criminal activity. At the same time, the rapid expansion of interconnected ALPR networks has generated significant privacy concerns because the systems collect information about overwhelmingly law-abiding motorists and can potentially be used to reconstruct a person's movements over days, weeks or months.

Illinois already regulates some aspects of ALPR use. The Illinois Vehicle Code prohibits certain sharing of ALPR information for immigration enforcement and investigations involving lawful reproductive and other health care. The Illinois State Police also operates cameras under the Expressway Camera Act, with statutory and administrative restrictions governing the program. However, Illinois does not yet have a comprehensive statewide law establishing uniform rules for every state and local law-enforcement agency concerning permissible searches, retention periods, audits, procurement, public disclosure and access to privately operated ALPR networks. Several bills introduced during the 2026 legislative session would establish substantially broader statewide standards.

The policy debate is consequently shifting from whether law enforcement should be permitted to use ALPRs toward **what safeguards should accompany their use**.

What Are Automatic License Plate Readers?

An ALPR is a camera combined with software capable of recognizing characters appearing on vehicle license plates and converting those images into searchable information. Cameras may be mounted on police vehicles or installed at fixed locations such as intersections, highways and entrances to communities.

Illinois law currently defines an ALPR as an electronic device mounted on a law-enforcement vehicle or positioned at a stationary location that can record or photograph a vehicle or license plate and compare the information with law-enforcement databases. Importantly, the Illinois definition also encompasses privately owned or operated readers when the information they collect is shared with law enforcement.

An individual ALPR detection can reveal relatively little: essentially that a particular vehicle was observed at a particular location at a particular time. The capabilities change considerably, however, when thousands of

cameras feed millions or billions of observations into searchable databases. Investigators can potentially enter a license plate and identify multiple locations where the vehicle was previously observed.

Modern systems may also record vehicle characteristics such as make, model and color. Some systems can identify other visual characteristics of vehicles, potentially allowing searches even when investigators do not know the precise license plate.

Growth of ALPR Networks

ALPR technology has moved rapidly from a specialized police tool to a widely distributed surveillance network. Cameras are increasingly operated not only by state and local police agencies but also by private vendors, businesses, homeowners associations and other private entities whose information may subsequently be accessible to law enforcement.

Flock Safety, one of the largest private ALPR vendors, was reported in August 2026 to operate a network exceeding 120,000 cameras nationally. The company operates in 49 states.

The significance of this growth is not simply the number of cameras. Networked technology allows information collected by one jurisdiction to potentially be searched by another jurisdiction hundreds or thousands of miles away. Consequently, a local government's decision to install several cameras can potentially contribute information to a much larger interstate surveillance system.

This interconnectedness has become one of the principal issues driving state legislative interest in ALPR regulation.

Public-Safety Applications

Law-enforcement agencies contend that ALPRs substantially improve their ability to locate vehicles connected with crimes or emergencies. The Illinois State Police states that its cameras compare license plates against databases including the National Crime Information Center and Illinois' Law Enforcement Agencies Data System. The technology can assist with missing-person investigations, AMBER Alerts, persons in crisis and vehicles connected to felony crimes.

ALPR systems can be particularly valuable when officers have only a vehicle description or license plate associated with an incident. Rather than relying exclusively upon officers to encounter the vehicle, the system can notify investigators when a camera identifies a potential match.

Historical ALPR information can also assist investigators in determining where a suspect vehicle traveled before or after an incident.

The technology therefore differs from traditional traffic cameras whose primary purpose may be traffic enforcement. ALPR systems function primarily as searchable investigative databases.

Existing Illinois Law

Illinois has adopted several laws relevant to ALPRs, although those laws do not yet constitute a comprehensive statewide regulatory framework.

Illinois Vehicle Code

Section 2-130 of the Illinois Vehicle Code expressly regulates ALPR information.

The statute prohibits an ALPR user from selling, sharing, transferring or allowing access to Illinois ALPR information to another state or local jurisdiction for the purpose of enforcing laws that interfere with lawful reproductive or other health-care services or that permit detention or investigation based upon immigration status.

Illinois ALPR users also may not provide information to an out-of-state law-enforcement agency unless that agency first provides a written declaration stating that the information will not be used for those prohibited purposes.

The protections apply broadly. The statutory definition of an ALPR user includes a person or entity operating the device, meaning that private companies sharing ALPR information with law enforcement may fall within the law.

These provisions became particularly significant following controversies involving searches of Illinois ALPR databases by agencies outside Illinois.

In 2025, the Illinois Secretary of State reported that a Texas law-enforcement agency had accessed Illinois ALPR information while investigating a woman who had obtained an abortion. The Secretary of State subsequently reported that 46 out-of-state agencies had conducted searches that violated Illinois requirements and that Mount Prospect's system had been searched hundreds of times for immigration-related purposes.

Later that year, the Secretary of State announced that audits identified additional improper access by U.S. Customs and Border Protection through ALPR systems operated by Flock Safety and Motorola Solutions. State officials directed that the access be disabled.

These incidents demonstrate one of the central policy challenges surrounding networked ALPR systems: **a local agency may collect the information, but the consequences of sharing that information can extend far outside that jurisdiction.**

The Expressway Camera Act

Illinois also regulates the Illinois State Police expressway camera network under the Expressway Camera Act.

The Illinois State Police reports that its ALPR records contain vehicle and license-plate images along with associated information including date, time and GPS coordinates. ISP currently maintains these records in its Vehicle Manager system for 90 days. Access is restricted to law-enforcement purposes, dissemination to other law-enforcement agencies is subject to restrictions, and departmental audits are conducted monthly.

ALPR information collected by ISP is also presently exempt from disclosure under the Illinois Freedom of Information Act. Current law provides that the FOIA exemption is scheduled to become inoperative July 1, 2028.

Public Act 104-18, enacted in 2025, extended and modified provisions of the Expressway Camera Act and related FOIA protections.

Broader Illinois Legislation Considered in 2026

The General Assembly considered several proposals during the 2026 session that illustrate how Illinois policy could evolve.

HB 5151 and its Senate counterpart SB 3816 proposed creating an Automated License Plate Recognition System Act. The proposal is considerably broader than existing Illinois law and would regulate ALPR technology operated by state and local governmental entities as well as certain privately operated systems whose information is available to government.

Among other provisions, the legislation would establish permitted and prohibited uses, retention requirements, restrictions on data sharing, security standards, audit requirements, public reporting and procedures governing access to historical information.

The proposal would require a government entity contemplating ALPR use to present the proposal publicly and provide an opportunity for comment before implementation. Agencies would be required to maintain written policies describing the purposes of the system, authorized personnel, retention periods, information-security protections, training and auditing procedures.

It would also prohibit combining ALPR systems with facial-recognition or other biometric technology and impose significant restrictions on immigration-related surveillance and surveillance associated with lawful health-care activities.

SB 3816 was re-referred to the Senate Assignments Committee on May 22, 2026, and had not been enacted as of August 18, 2026.

Other legislation has proposed somewhat different regulatory approaches. HB 5231, for example, would establish agency policies and reporting requirements and provide that an ALPR notification alone would not constitute reasonable suspicion sufficient to stop a vehicle. It would also establish criminal penalties for certain intentional misuse of ALPR information.

SB 3257 takes a different approach to retention. It proposes allowing law-enforcement agencies to retain ALPR records for as long as five years while requiring records to be archived after 90 days, restricting access to older records and preventing out-of-state agencies from searching archived information.

These competing approaches illustrate one of the fundamental unresolved questions before Illinois policymakers: **whether historical ALPR information should be quickly deleted or retained for potentially valuable future investigations.**

Regulation in Other States

State approaches vary considerably.

The National Conference of State Legislatures (NCSL) reports that at least 18 states have enacted laws addressing ALPR use or retention of ALPR information. Earlier NCSL research specifically identified statutes in Arkansas, California, Colorado, Florida, Georgia, Maine, Maryland, Minnesota, Montana, Nebraska, New Hampshire, North Carolina, Oklahoma, Tennessee, Utah and Vermont.

More states have subsequently enacted legislation.

Virginia enacted a comprehensive ALPR statute in 2025. Its law restricts law-enforcement searches to specified investigative purposes, generally requires ALPR information to be deleted after 21 days, requires audit trails, limits sharing, requires agency policies and public reporting, and provides that an ALPR alert alone does not automatically justify a vehicle stop.

Washington enacted comprehensive legislation in 2026. Among other requirements, Washington prohibits agencies from selling ALPR information, restricts interagency access, generally requires warrants to obtain privately held ALPR information and requires vendors to implement technical controls preventing unauthorized sharing.

Although the details vary substantially, state statutes generally address one or more recurring issues:

- **Permissible purposes.** Some states restrict ALPR searches to criminal investigations, stolen vehicles, missing persons or other specifically defined public-safety purposes.
- **Retention periods.** States have adopted retention periods ranging from minutes or weeks to months or years.
- **Data sharing.** Some states restrict sharing with private companies, federal agencies or other jurisdictions.
- **Auditing and accountability.** Agencies may be required to record who searched a database, which plate was searched and the reason for the search.
- **Public reporting.** Some laws require agencies to disclose the number of cameras, searches, alerts or investigations involving ALPRs.
- **Public-record protections.** Many states exempt raw ALPR information from open-records laws because releasing vehicle-location histories publicly could itself create privacy and safety concerns.
- **Vendor regulation.** More recent statutes increasingly regulate the private companies that store and operate ALPR databases rather than focusing exclusively on police departments.

This last development is especially important because ALPR systems increasingly operate as public-private information networks rather than stand-alone police cameras.

Privacy Concerns

ALPRs create an unusual privacy question because the information captured at any single moment is generally visible to anyone standing along a public roadway.

Drivers ordinarily do not have a reasonable expectation that their license plates will remain private while traveling publicly. The more difficult question is whether the government should be permitted to collect millions of individual observations, retain them and use computers to reconstruct people's movements.

Tracking Innocent Individuals

ALPR systems record vehicles without first determining whether their occupants are suspected of wrongdoing.

Consequently, most information stored in an ALPR database involves individuals who are not suspected of committing a crime.

This creates what privacy scholars sometimes describe as a distinction between **observation** and **persistent surveillance**. An officer seeing a vehicle drive down a street presents little privacy concern. A computer database capable of determining where that same vehicle traveled repeatedly over several months presents a different question.

Patterns of movement may indirectly reveal sensitive information. Regular visits to a medical facility, political organization, religious institution, substance-abuse treatment facility, domestic-violence shelter or particular person's residence can potentially reveal considerably more than a license plate itself.

Retrospective Surveillance

Traditional surveillance generally requires law enforcement to decide whom to monitor before the surveillance occurs.

ALPR databases reverse that sequence.

Because information is collected continuously, investigators may be able to select a person today and reconstruct where that person's vehicle traveled weeks earlier.

The Illinois State Police currently retains its ALPR information for 90 days, for example.

The longer information is retained and the more cameras participate in a searchable system, the more complete this retrospective picture can become.

Interstate and Federal Data Sharing

Illinois' experience demonstrates another concern.

ALPR information collected under Illinois law can potentially be accessed by law-enforcement agencies operating under substantially different state policies. The 2025 Illinois incidents involving abortion and immigration investigations demonstrated how local databases can effectively become part of national surveillance networks.

Privacy therefore depends not only upon the rules imposed by the government that owns the camera, but also upon contractual settings, vendor architecture and permissions governing thousands of potential users.

Private ALPR Networks

Private-sector ALPR systems present additional legal questions.

A police department directly operating a camera is clearly a government actor subject to constitutional and statutory constraints. A private company photographing vehicles traveling on public roads may occupy a substantially different legal position.

The distinction becomes blurred when government agencies purchase access to enormous databases compiled by private companies.

Rather than deploying surveillance equipment itself, an agency can potentially purchase access to vehicle-location information already collected by third parties. Some states, including Washington and Utah, have therefore imposed special restrictions on government access to privately held ALPR information.

Accuracy and False Matches

ALPR technology is not infallible.

A plate may be misread because of lighting, weather, camera angle, plate damage or similar characters. Databases against which plates are compared also may contain outdated information.

For that reason, policymakers increasingly distinguish between an **ALPR alert** and independent evidence establishing reasonable suspicion or probable cause.

Virginia's statute, for example, provides that a notification alone does not constitute reasonable suspicion and requires additional confirmation before a vehicle stop. Similar language has been proposed in Illinois.

Constitutional Questions

The Fourth Amendment question surrounding ALPR technology remains important but evolving.

A federal district court considering Illinois' system in *Scholl v. Illinois State Police* rejected a constitutional challenge in 2025. The court concluded that Illinois' existing ALPR program was not sufficiently comprehensive to constitute a Fourth Amendment search.

The court emphasized that license plates and vehicle movements on public roadways generally carry reduced expectations of privacy. At the same time, the court expressly declined to decide whether a more extensive ALPR network could eventually cross the constitutional line.

That distinction could become increasingly important as camera networks expand.

The U.S. Supreme Court has recognized in other digital-location cases that the aggregation of extensive location information can implicate privacy interests even when individual observations might not. In its June 2026 decision in *Chatrue v. United States*, the Court again considered the constitutional significance of highly detailed historical digital-location information in light of its earlier decision in *Carpenter v. United States*.

Thus, existing precedent should not necessarily be interpreted as establishing that every future ALPR network will automatically be constitutionally permissible. The scale, duration, comprehensiveness and method of accessing stored information may matter.

Key Policy Questions for Illinois Counties

ALPRs present counties with both an operational opportunity and a governance responsibility.

County boards and sheriffs considering the technology should recognize that procurement decisions can establish long-term surveillance infrastructure. Contracts should therefore address not only price and camera performance but also ownership of information, retention schedules, cybersecurity, audit trails, vendor access, secondary use and interstate data sharing.

Several questions merit particular attention:

1. **What crimes or circumstances justify searching historical ALPR information?**
2. **How long should information concerning vehicles with no connection to criminal activity be retained?**
3. **Who should be permitted to search the database?**
4. **Should every search require a documented case number and investigative purpose?**
5. **Should another agency automatically receive access to locally collected information?**
6. **What restrictions should apply to federal or out-of-state agencies?**

7. **Should historical searches extending beyond a specified period require supervisory approval, a court order or a warrant?**
8. **What audit procedures should identify improper searches?**
9. **What information should local governments publicly report without disclosing sensitive investigative information?**
10. **What contractual obligations should apply to private ALPR vendors concerning data ownership, retention, cybersecurity and disclosure?**

Policy Considerations

A balanced Illinois framework need not require policymakers to choose between unrestricted surveillance and eliminating ALPR technology.

The strongest regulatory models preserve legitimate investigative uses while establishing safeguards around the enormous volume of information concerning people who have no connection to criminal activity.

A comprehensive framework could include a relatively short default retention period for routine detections while permitting longer preservation when information is connected to an identified investigation. Searches could require documented investigative purposes, authenticated users and automatic audit trails. Agencies could conduct routine audits and impose penalties for intentional misuse.

State law could also establish clear rules governing vendor contracts and cross-jurisdictional sharing. This is increasingly important because technological controls established by vendors can sometimes determine practical access to information more effectively than written agency policies.

Finally, Illinois policymakers may wish to distinguish between **real-time alerts** and **historical searches**. Using a camera to identify a stolen vehicle currently passing an intersection creates different privacy implications than searching months of historical information to determine everywhere a particular vehicle has traveled. Different levels of legal authorization could therefore reasonably apply to these two uses.

Conclusion

Automatic license plate readers have become powerful investigative tools, and their use is likely to continue expanding. Their effectiveness derives largely from their ability to transform millions of otherwise fleeting observations into searchable vehicle-location information.

That same capability creates the central privacy concern.

The important policy question is therefore no longer simply whether a license plate is visible on a public street. It is whether government agencies should be able to systematically collect, retain, combine and search those observations to reconstruct people's movements, and, if so, under what conditions.

Illinois has already established important restrictions, particularly concerning interstate sharing for immigration and lawful health-care investigations, and the State Police program operates under additional statutory and administrative safeguards. Nevertheless, the state continues to debate broader standards applicable to local law enforcement, private vendors and interconnected ALPR databases.

For counties, the emerging policy objective should be to preserve the legitimate public-safety value of ALPR technology while establishing clear limitations on purpose, retention, access, sharing and accountability. Doing so can provide law enforcement with a useful investigative tool without allowing a collection of local

cameras to evolve, largely by default, into an unrestricted system for tracking the movements of Illinois residents.

