

Federal Legislation and Oversight of Law Enforcement Use of Automated License Plate Readers (ALPRs)

September 3, 2026

Law enforcement use of automated license plate readers (ALPRs) is [relatively commonplace in many jurisdictions](#). Law enforcement agencies use ALPRs for a variety of proactive and reactive policing purposes, including gathering intelligence and evidence, helping identify potential suspects, and facilitating crime scene analysis. Use of ALPRs by law enforcement has come under heightened scrutiny following [reports of their misuse](#). This Insight outlines how ALPRs may be used by law enforcement and highlights legislative proposals the 119th Congress and possible issues for congressional oversight of this technology.

How ALPRs Work

ALPR systems work by automatically capturing images or videos of passing vehicles. A computer algorithm then detects, reads, and converts the license plate characters within the image into readable data. ALPR technology can also identify and retain associated information in the images, including vehicle type and color, global positioning system (GPS) location data, and date and time. Individuals in the images/videos collected with ALPRs may also be able to be identified using facial recognition technology (FRT). ALPR systems allow law enforcement to compare data from the images/videos against various databases, including [hot lists](#) that contain license plates linked to vehicles of interest and alert an officer when there is a match. Data retained from ALPR systems may also help law enforcement track vehicle location over time, depending on agencies' data collection, retention, and sharing policies.

ALPR Use by Law Enforcement

According to the Bureau of Justice Statistics, larger law enforcement agencies are more likely to use ALPR technology than smaller agencies—[nearly 90% of sheriffs' offices](#) with 500 or more sworn deputies, compared to 20% of all sheriffs' offices regardless of size, and [100% of police departments serving over 1 million residents](#), compared to nearly 22% of all police departments regardless of size, reported using the technology. ALPRs are used by public safety and private entities alike. One of the

Congressional Research Service

<https://crsreports.congress.gov>

IN12735

largest networks of ALPRs in the country is produced by [Flock Safety](#). At the end of August 2026, [crowdsourced data](#) from an [advocacy organization](#) had mapped over 137,000 ALPR cameras across the United States, with over 80% attributed to Flock Safety.

[Information collected](#) by ALPRs may be maintained in public or private systems, accessible to or searchable by law enforcement. It is the data retention and database searchability aspects of ALPR systems that have come under [particular scrutiny](#). Concerns over law enforcement misuse of these systems—including to carry out [criminal activity such as stalking](#) and the potential for government surveillance of individuals captured in the data collected, retained, and shared by these systems—have been in the spotlight. These concerns have led Flock Safety, for example, [to update](#) its “privacy, accountability, security, and transparency safeguards,” though [some have questioned](#) whether these changes will have substantive effects on data privacy. These surveillance-related concerns have also led to [some jurisdictions](#) to [ending their contracts](#) with ALPR vendors, and to debates over whether Congress should take a more direct role in this space.

Legislation and Oversight of ALPR Use by Law Enforcement

There is no specific federal legislative framework that governs law enforcement use of ALPRs; rather, there are federal laws and policies broadly governing law enforcement investigations and intelligence gathering. There is also a [patchwork of state laws and policies](#) on ALPR use.

In the 119th Congress, legislation has been introduced to affect ALPR use from various angles, including the following:

- H.R. 9800 would, among other things, prohibit federal agencies from purchasing, deploying, operating, accessing, or contracting with automated surveillance systems that can identify, track, or record individuals, including ALPR systems—and specifically, Flock Safety cameras. It would also prohibit state, local, and tribal government entities from using federal funds for these purposes. It would require federal agencies that violate this prohibition to delete the associated data within 30 days and would prohibit those data from being used in a court or administrative proceeding.
- H.R. 9716 would, among other things, require the Attorney General to maintain a list of surveillance devices and related technologies, including ALPR systems, used by state and local law enforcement agencies. It would also establish that federal law enforcement agencies could not access the associated data without a warrant from a federal judge. Additionally, it would establish bounds on retention of these data by federal law enforcement once they access it.
- H.R. 8470 would, among other things, require law enforcement to obtain a warrant for searches of certain third-party data, metadata, and personal information. It would provide exceptions to this warrant requirement but would not include access to ALPR and similar data in these exceptions.
- Congress has also looked to condition federal funding on ALPR use. For instance, an [amendment](#) offered to H.R. 8870 would have prohibited the use of ALPRs by entities receiving federal highway funding.
- Other legislation on license plate readers has focused on U.S. Customs and Border Protection (CBP) activities at the border. For instance, S. 3997 and H.R. 1678 would require reporting on data collection activities at CBP checkpoints, including on the use of license plate readers. Additionally, H.R. 9199 would require CBP to upgrade license plate readers at the ports of entry.

Some policymakers have also initiated congressional investigations into ALPR systems, chiefly to gather information about their data collection and sharing activities. If Congress continues its oversight efforts, policymakers may examine how potential boundaries on ALPR use and data sharing might apply, as well as internal ALPR policies federal law enforcement agencies may have developed and maintained to govern their use of the technology. Congress may also elect to assess the adequacy of ALPR information in federal agencies' Privacy Impact Assessments and Systems of Records Notices, or may provide guidance on when, and under what circumstances, federal grant programs may be used to support state and local law enforcement use of ALPRs.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.