LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION

AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS

DECEMBER 2025

INTRODUCTION

Automatic license plate recognition systems (ALPRs)[1] "are camera systems that capture license plate data of vehicles"[2] and are available in fixed, mobile, and portable applications.[3] Fixed cameras are those cameras that are mounted to a fixed location, typically using existing infrastructure (*e.g.*, light poles, traffic lights, and public or private buildings).[4] Mobile systems are typically mounted on police or private contracted vehicles such as tow trucks and taxis, while portable systems are those cameras that are not mounted to a vehicle but can be moved from location to location, such as a "quick-deploy" camera or an ALPR "trailer" that may also capture a vehicle's speed.[5]

ALPR systems automatically capture images or videos of all vehicles that pass the camera if the system algorithm detects what it determines to be a license plate.[6] A computer algorithm then converts the image or video into readable-data, that includes the license plate number and any additional information that the system is set up to detect including, but not limited to, global positioning system (GPS) location data for the camera that took the photograph or video; vehicle make, model, and color; date and time; and other information such as the name of the agency that owns or operates the system and site identification.[7] Once the information has been captured and cataloged by the ALPR system, the system can then compare those "data points against various databases, including 'hot lists,' which contain a list of license plates linked to vehicles of interest. If there is a match to a 'hot list' license plate, the ALPR system can alert a law enforcement officer in real time."[8] A "hot list" is a list of license plate characters associated with vehicles of interest and may also include information on vehicles that originally appear on a "be on the lookout" (BOLO) list[9] and can also include information on vehicles related to kidnappings, AMBER alerts, stolen vehicles, drug-related cases, and other criminal activities including potential terrorist activity.[10] In addition to unsolicited notifications from an ALPR system, law enforcement users can manually query the system for investigative purposes.[11] Depending on the system, ALPR data may be queried

[1] Automatic license plate recognition systems are known by a variety of other names including license plate readers, automatic or automated number plate recognition systems, automatic license plate recognition technology, automatic vehicle identification, car plate recognition, and vehicle license plate recognition or identification systems.

[2] Peter G. Berris, Kristin Finklea, and Dave S. Sidhu, *Automated License Plate Readers: Background and Legal Issues*, Cong. Rsch. Serv. 1 (July 21, 2025), https://www.congress.gov/crs-product/IF13068.

[3] *Id. See also* Colin L. Drabert, "Law Enforcement Use of Technology: Automatic License Plate Recognition (ALPR)," presented at the Virginia State Crime Commission, Nov. 14, 2024, https://studiesvirginiageneralassembly.s3.amazonaws.com/meeting_docs/documents/000/002/458/original/VSCC_ALPR_Dec_3_JCOTS.pdf?1733235622.

[4] Berris et al., *supra* note 2.

[5] *Id. See also* Drabert, *supra* note 3 and *Northern California Fusion Center has 3 Covert ALPR Trailers to Loan Out*, The Ctr. for Hum. Rts. and Priv., https://www.cehrp.org/tags/lpr-speed-trailer/.

[6] Berris et al., *supra* note 2.

[7] *Id*. Note that most ALPR systems are predominantly installed to capture rear license plate data and, although it may occur in practice, capturing images of drivers and/or passengers is accidental and not the intended purpose of the system.

[8] *Id*.

[9] "'BOLO' or 'Be on the Lookout' refers to a determination by a law enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle." *Automatic License Plate Reader (ALPR)*, Grandview Heights Police Gen. Ords. (rev. May 9, 2022), https://grandviewheights.gov/DocumentCenter/View/7126/391-Automatic-License-Plate-Reader#:~:text=Definitions%20and%20Acronyms,or%20locate%20a%20particular%20vehicle.

[10] Kristin Finklea, *Law Enforcement and Technology: Use of Automated License Plate Readers*, Cong. Rsch. Serv. 1-2 (Aug. 19, 2024), https://www.congress.gov/crs-product/R48160.

[11] Berris et al., *supra* note 2.

using a full or partial license plate number, a description of the vehicle, and by querying the license plate characters or vehicles that appear in a similar location during the same timeframe.[12]

In addition to finding vehicles that appear on hot lists, ALPR data is also used by government entities for enforcement of parking laws, toll collection, and analysis of traffic patterns.[13] Private individuals and entities also use ALPR systems for a range of commercial purposes as well as for neighborhood and home security purposes. Non-governmental use of ALPR systems includes parking enforcement in private lots and by homeowners' associations, consumer marketing, enabling repossession of vehicles with past-due car loans where the lender has a contractual right to repossess a vehicle, and investigating insurance fraud.[14]

The use of ALPR systems, particularly by law enforcement entities, is prevalent throughout the United States. According to a 2020 survey conducted by the Bureau of Justice Statistics, U.S. Department of Justice, nearly 90 percent of sheriffs' offices with 500 or more sworn officers reported using ALPRs, while 100 percent of those police departments serving more than one million residents reported ALPR use.[15] Federal law enforcement agencies like the Federal Bureau of Investigation, the U.S. Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives also use ALPR technology in performing their law enforcement duties.

The Drug Enforcement Administration (DEA) administers the National License Plate Reader Program (NLPRP), the data from which is shared with state and local law enforcement agencies who have signed memoranda of understanding with the DEA.[16] The DEA uses the NLPRP to "[facilitate] the investigation of drug trafficking, bulk cash smuggling and other illegal activities associated with the drug trade."[17] ALPR cameras used by the DEA are placed along known high-level drug and money trafficking public roadways and can be connected to other ALPR systems operated by other federal agencies as well as state, local, and tribal law enforcement entities.[18] DEA officers and law enforcement officers at partner agencies can access the NLPRP system through the DEA Special Intelligence Link to support their drug-related and other criminal investigations.[19]

REGULATION OF ALPRS

As of September 2025, 23 states, the District of Columbia, and the U.S. Virgin Islands have statutes and/or administrative rules in place that regulate the use of ALPRs.[20] The laws in 16 states, [21] the District of Columbia, and the U.S. Virgin Islands regulate use by at least one governmental entity, including law enforcement, while the laws in Arkansas, California, Illinois, and Tennessee apply to both governmental entities and private individuals

[12] Drabert, *supra* note 3.

[13] *Automatic License Plate Recognition Systems: Summary of State Laws*, LEGIS. ANALYSIS & PUB. POL'Y ASS'N (Sept. 2025), Automatic License Plate Recognition Systems: Summary of State Laws | LAPPA.

[14] *See* Ángel Díaz and Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use,* BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.

[15] *Sheriffs' Offices, Procedures, Policies, and Technology, 2020 – Statistical Tables, Table 14*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS, BUREAU OF JUST. STAT. 23 (Nov. 2023), Sheriffs' Offices, Procedures, Policies, and Technology, 2020 – Statistical Tables and *Local Police Departments, Procedures, Policies, and Technology, 2020 – Statistical Tables, Table 14*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS, BUREAU OF JUST. STAT. 22 (Nov. 2023), Local Police Departments, Procedures, Policies, and Technology, 2020 – Statistical Tables.

[16] *Privacy Impact Assessment for the National License Plate Reader Program (NLPRP) and DEA Special Intelligence Link (DEASIL)*, U.S. DEP'T OF JUST., DRUG ENF'T ADMIN. 11 (Dec. 20, 2024), Privacy Impact Assessment.

[17] *Id*. at 1.

[18] *Id*.

[19] *Id*. at 2.

[20] LAPPA, *supra* note 13.

[21] The 12 states are Alabama, Colorado, Florida, Georgia, Idaho, Kansas, Maine, Maryland, Montana, Nebraska, New Hampshire, North Carolina, Oklahoma, Utah, Vermont, and Virginia.

or entities. Pursuant to Maine law, with the exception of the state department of transportation; the department of public safety, bureau of state police; and any state, county, or municipal law enforcement agency, "a person may not use an automated license plate recognition system" making it the only state that does not permit use by private individuals.[22]

Most ALPR laws regulate who can access ALPR data and the purposes for which that data can be accessed; how long ALPR data can be retained; the keeping of logs related to ALPR access, querying, and dissemination; data preservation requirements; audit requirements; the requirement that governmental entities have written policies and procedures in place for their employees related to ALPR systems; reporting requirements; and civil and/or criminal penalties for violating the law.

In some states with ALPR laws, ALPR data held by law enforcement can be shared with other governmental entities, including other law enforcement agencies; however, some states and entities allow broader sharing (*e.g.*, with federal and/or out-of-state law enforcement agencies) or place limits on data sharing.[23] For example, in New Jersey, in-state sharing of ALPR data is mandatory for all law enforcement agencies, but data sharing agreements must be in place to share data with out-of-state law enforcement agencies.[24] By contrast, Virginia does not permit law enforcement agencies not located within the commonwealth to access ALPR data.[25] See Automatic License Plate Recognition Systems: Summary of State Laws for more information, including state-by-state tables.

PRIVACY CONCERNS

Opponents of ALPR use by law enforcement argue that it infringes on the Fourth Amendment prohibition against unreasonable searches and seizures. For purposes of the Fourth Amendment, a "search" involves either "(1) government intrusion upon a person's reasonable expectation of privacy, or (2) government trespass upon a constitutionally protected space."[26] If law enforcement conducts a search, courts then ask whether the officer had a warrant and, if not, whether an exception to the warrant requirement applies.[27] There are three primary doctrines or theories to which the courts have turned to determine whether ALPR use by law enforcement might implicate the Fourth Amendment: (1) the plain view doctrine; (2) the third-party doctrine; and (3) mosaic theory.

The U.S. Supreme Court noted the "plain view" exception to the warrant requirement in the 1967 case of *Katz v. United States*.[28] The issue in *Katz* was whether law enforcement required a warrant to conduct electronic surveillance of a public telephone booth, a question that the Court answered in the positive.[29] In its opinion, the Court specifically stated that, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection … But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[30] In other words, if an object is in plain view, an individual does not have an expectation of privacy in that object, and the Fourth Amendment protections are not triggered unless the individual has taken measures to ensure privacy. In *Katz*, the Court found that, although the phone booth was partially constructed of glass and, therefore, open to public view, Katz did not lose his right to keep his conversation private simply because he could be observed.[31]

[22] ME. REV. STAT. ANN. tit. 29-A, § 2117-A (West 2025).
[23] LAPPA, *supra* note 13.
[24] *Attorney General Law Enforcement Directive No. 2022-12*, OFC. OF THE ATT'Y GEN. 6 (Oct. 21, 2022), ag-Directive-2022-12_Updated-Directive-Regulating-Use-of-Automated-License-Plate-Recognition-(ALPR)-Technology.pdf.
[25] VA. CODE ANN. § 2.2-5517 (West 2025).
[26] Berris et al, *supra* note 2.
[27] *Id.*
[28] Katz v. United States, 389 U.S. 347 (1967).
[29] *Id.* at 359.
[30] *Id.* at 351 (citations omitted).
[31] *Id.* at 352.

Over the years, the Court has expanded on what constitutes a reasonable expectation of privacy. The cases of *United States v. Miller*[32] and *Smith v. Maryland*[33] are often cited as the bases for what is known as the "third-party doctrine." In broad terms what the third-party doctrine says is that a person does not have a legitimate or reasonable expectation of privacy in information provided to a third party and, therefore, law enforcement is not required to obtain a warrant to access certain information conveyed to that third party. In *Smith*, the Court stated that it:

> uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action. This inquiry … normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy … The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[34]

The Supreme Court applied the third-party doctrine to traveling on public roads in the case of *United States v. Knotts*[35] in which Knotts and his co-defendants were arrested for manufacturing controlled substances. Law enforcement suspected that one of the defendants was purchasing chloroform to use in the manufacture of controlled substances. With the consent of the seller, law enforcement placed a beeper in a container of chloroform that had been sold to the co-defendants and then followed the signal to Knotts' home through both visual and electronic methods. The officers secured a warrant to search the premises and discovered a drug laboratory. At trial, Knotts argued that he had a reasonable expectation of privacy in his home and that the use of the beeper to track the chloroform container without a warrant violated the Fourth Amendment. In its analysis of the case, the Court found that the surveillance conducted "amounted principally to the following of an automobile on public streets and highways."[36] The Court then stated: "A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[37] Even though Knotts was not the driver of the vehicle, he could not claim a reasonable expectation of privacy in the "visual observation of [co-defendant's] automobile arriving on his premises after leaving a public highway…."[38]

Taken together, the third-party and plain view doctrines seem to indicate that law enforcement is not required to obtain a warrant in order to use ALPR systems to identify suspect vehicles. However, using ALPR data to track a suspect vehicle over an extended period of time *might* trigger the Fourth Amendment warrant requirement. In *Carpenter v. United States*, the Supreme Court held that law enforcement must obtain a warrant in order to access

[32] 425 U.S. 435 (1976). Miller contended that he had a reasonable expectation that his bank records would be kept private. The Court disagreed, finding that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id*. at 443.

[33] 442. U.S. 735 (1979). Smith was arrested for robbery after law enforcement obtained records of phone numbers dialed from his home telephone that indicated he was the person making threatening phone calls to the victim. Smith argued that he had a reasonable expectation of privacy in keeping the numbers dialed private. The Court held that because telephone numbers are conveyed to the telephone company (*i.e.,* a third party) and telephone subscribers are aware that the telephone company keeps records of the numbers dialed, there is no legitimate expectation of privacy in those records.

[34] *Id*. at 740 (internal citations omitted).

[35] 460 U.S. 276 (1983).

[36] *Id*. at 281.

[37] *Id*.

[38] *Id*. at 282.

cell-site location information (CSLI).[39] As explained in the opinion, cell phones continuously scan for the best signal, typically the closest cell site to the phone's location. Every time the phone connects to a specific cell site, a time-stamped record – the CSLI – is generated. During its investigation into a series of robberies, law enforcement obtained CSLI on Carpenter for a period of 127 days comprising almost 13,000 location points "cataloging Carpenter's movements."[40] Based on this data, police officers were able to put Carpenter in the location of each of the robberies being investigated. The Sixth Circuit Court of Appeals held that Carpenter lacked a reasonable expectation of privacy in his location information because that information was shared with his cell phone carrier.[41] The Supreme Court reversed that decision, stating that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[42] Additionally, the Court declared that individuals do not "surrender all Fourth Amendment protection by venturing into the public sphere."[43] The Court went on to say:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." […] And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.[44]

The Court further distinguished vehicles from cell phones, stating: "[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[45]

The idea that "prolonged surveillance may give law enforcement a larger and more intimate picture of a person's life and may breach a reasonable expectation of privacy, necessitating a warrant" is known as the mosaic theory.[46] It is this theory that leads some experts to believe that sustained tracking of a particular suspect vehicle through ALPR technology or using ALPR systems in concert with other surveillance tools may trigger Fourth Amendment protections.[47]

As of December 2025, no federal appellate court has found that law enforcement use of ALPR systems violates the Fourth Amendment.[48] However, these cases tend to be very fact specific – that is, courts have generally

[39] 585 U.S. 296 (2018).

[40] *Id*. at 301.

[41] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), reversed.

[42] U.S. v. Carpenter, 585 U.S. 296, 309 (2018).

[43] *Id*. at 310.

[44] *Id*. at 311.

[45] *Id*.

[46] Berris et al, *supra* note 2.

[47] *Id*.

[48] Note, however, that of the three federal appeals court opinions located by the drafters of this fact sheet, none of the courts reached the potential Fourth Amendment implications of law enforcement's use of ALPR technology. In each case, the court upheld the use of ALPR technology on other grounds. United States v. Mapson, 96 F.4th 1323 (11th Cir. 2024) (the court held that because law enforcement accessed ALPR data on the defendant's vehicle the day before the *Carpenter* decision was handed down, and the "Supreme Court has held that '[e]vidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule,'" police officers were authorized under binding precedent to access the ALPR data without a warrant); United States v. Yang, 958 F.3d 851 (9th Cir. 2020) (finding that the defendant did not have a reasonable expectation of privacy in the historical location data of the vehicle at issue under the facts of this case); and Green v. City and County of San Francisco, 751 F.3d 1039 (9th Cir. 2014) (the question at issue in this case was whether the traffic stop of Green's vehicle based on erroneous data from an ALPR system was a seizure within the meaning of the Fourth Amendment).

declined to apply *Carpenter* due to the specific facts of each case. For example, in *United States v. Martin*, the District Court distinguished *Carpenter* from the facts in *Martin* on the basis that retrieving only three photographs of Martin's vehicle over a 30-day period "did not allow law enforcement to track or monitor the 'whole of [his] physical movements,' and therefore was not a search under the Fourth Amendment."[49] The court noted that "tracking a cellphone's location 'achieves near perfect surveillance' equivalent to 'attach[ing] an ankle monitor to the phone's user,' which is not present when monitoring vehicular travel."[50]

The court also examined the case of *Leaders of a Beautiful Struggle v. Baltimore Police Department* where the Fourth Circuit Court of Appeals held "that government officials' warrantless access to an aerial surveillance system that allowed them to deduce that the 'whole of individuals' movements' constituted an unconstitutional search under the Fourth Amendment."[51] In reaching its decision in this case, the court noted both the Fourth Circuit's focus on the "prolonged tracking" involved in the *Leaders of a Beautiful Struggle* case and the "all-encompassing record" of Carpenter's movements in that case to determine that, under the facts in this case, the use of ALPR data to track Martin's movements was not a violation of his rights under the Fourth Amendment.[52] The court specifically limited its ruling to the facts in this case and refused to speculate about how and whether future developments in ALPR technology might change the analysis.[53]

CONCLUSION

ALPRs assist law enforcement and other governmental entities in identifying vehicles of interest and enforce municipal, county, and state laws. They also help locate missing people, stolen vehicles, and vulnerable adults. ALPR use is widespread, and their use is being challenged as an invasion of privacy in violation of the Fourth Amendment in lower courts across the country. As of the publication of this document, no federal court has found that accessing ALPR data is a violation of any person's Fourth Amendment rights.

ABOUT THE LEGISLATIVE ANALYSIS AND PUBLIC POLICY ASSOCIATION

The Legislative Analysis and Public Policy Association (LAPPA) is a 501(c)(3) nonprofit organization whose mission is to conduct legal and legislative research and analysis and draft legislation on effective law and policy in the areas of public safety and health, substance use disorders, and the criminal justice system.

LAPPA produces up-to-the-minute comparative analyses, publications, educational brochures, and other tools ranging from podcasts to model laws and policies that can be used by national, state, and local criminal justice and substance use disorder practitioners who want the latest comprehensive information on law and policy. Examples of topics on which LAPPA has assisted stakeholders include naloxone laws, law enforcement/community engagement, alternatives to incarceration for those with substance use disorders, medication for addiction treatment in correctional settings, and the involuntary commitment and guardianship of individuals with alcohol or substance use disorders.

For more information about LAPPA, please visit: https://legislativeanalysis.org/.

© Legislative Analysis and Public Policy Association - This project was supported by the Model Acts Program, funded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily reflect the official position or policies of the Office of National Drug Control Policy or the United States Government.

[49] United States v. Martin, 753 F.Supp.3d 454, 476 (E.D. Va. 2024).
[50] *Id.* at 465.
[51] *Id.* citing *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 333 (4th Cir. 2021).
[52] *Id.* at 471.
[53] *Id.*